UNIVERSIDADE FEDERAL DE SANTA CATARINA

ESPECIALIZAÇÃO EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO APLICADAS À SEGURANÇA PÚBLICA E DIREITOS HUMANOS

SAMUEL NUNES JULIANI

SOFTWARES FORENSES DIRECIONADOS À INVESTIGAÇÃO DE CRIMES VIRTUAIS EM REDES DE COMPUTADORES

Araranguá, 15 de Maio de 2017

SAMUEL NUNES JULIANI

SOFTWARES FORENSES DIRECIONADOS À INVESTIGAÇÃO DE CRIMES VIRTUAIS EM REDES DE COMPUTADORES

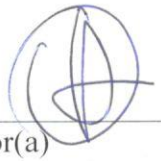
Trabalho de Conclusão de Curso submetido à Universidade Federal de Santa Catarina como parte dos requisitos necessários para a obtenção do Grau de Especialista em Tecnologias da Informação e Comunicação aplicadas à Segurança Pública e Direitos Humanos. Sob a orientação da Professora Dr.ª Eliane Pozzebon.

Araranguá, 2017

Samuel Nunes Juliani

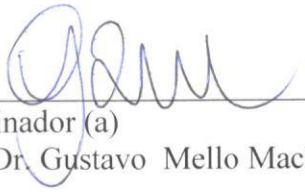
Título: "SOFTWARES FORENSES DIRECIONADOS À INVESTIGAÇÃO DE CRIMES VIRTUAIS EM REDES DE COMPUTADORES"

Trabalho de Curso submetido à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do Grau de Especialista em Tecnologias da Informação Comunicação aplicadas à Segurança Pública e Direitos Humanos.



Orientador(a)
Prof.ª Dr.ª Eliane Pozzebon/ UFSC

Examinador (a)
Prof.ª Dr.ª Luciana Bolan Frigo/UFSC



Examinador (a)
Prof. Dr. Gustavo Mello Machado/UFSC

Araranguá, 15 de maio de 2017

“Dedico este trabalho à minha família
pela compreensão e parcimônia durante todas
minhas conquistas”.

AGRADECIMENTOS

Presto meus agradecimentos a todas as pessoas e instituições que direta ou indiretamente contribuíram para a construção desse trabalho. No entanto, quero ressaltar meu agradecimento ao meu amigo William Schneider por ter contribuído com seus conhecimentos.

“É necessário cuidar da ética para não anestesiarmos a nossa consciência e começarmos a achar que tudo é normal. ”

Mário Sérgio Cortella

RESUMO

Com o crescimento e desenvolvimento da internet no mundo ligando por meio de uma gigantesca malha todas as pessoas e instituições, a segurança das informações passou a ser questionada bem como o surgimento de crimes no universo virtual e passou a necessitar de um tratamento diferenciado. A necessidade de criação de leis específicas, a padronização de métodos e formas de garantir a segurança na rede e uma ciência forense capaz de apontamentos precisos entraram em evidência para sobrepor esta violação em que a sociedade está sendo submetida. Desta forma, o presente estudo tem por objetivo definir redes de computadores colocando em evidência elementos que garantam a segurança das informações e também que afetam, mostrando a necessidade da tomada de boas práticas para a garantia da segurança na rede. Consequentemente, é tratado do ilícito ocorrido mediante a quebra da ordem no universo digital, evidenciando o conceito desse tipo de crime, legislações pertinentes e específicas e formas de investigação preventiva utilizadas pela polícia. Logo, mediante tal quebra de ordem, passa-se a fase de consubstanciação da ilicitude ocorrida, e é nesse ponto que ocorre a principalidade desse estudo, tornando evidente a perícia forense computacional como ciência exclusiva para obtenção de indícios criminosos dentro do ambiente virtual para confecção de laudos comprobatórios. E dentro desse nicho, como especificação do tema proposto, são destacadas algumas ferramentas voltadas a captura de dados direcionadores da investigação e perícia de crimes virtuais ocorridos dentro de redes de computadores.

Palavras-chave: Redes de computadores; Segurança da informação; Crime virtual; Perícia forense computacional.

ABSTRACT

With the growth and development of the Internet in the world linking through a gigantic network all people and institutions, information security began to be questioned as well as the emergence of crimes in the virtual universe and started to need a differential treatment. The need to create specific laws, the standardization of methods and ways to ensure network security, and a forensic science capable of precise notes have come in evidence to override this violation in which society is being subjected. In this way, the present study aims to define computer networks highlighting elements that guarantee information security and also that affect, showing the need to take good practices to guarantee network security. Consequently, it deals with the illegal occurrence through the breakdown of the order in the digital universe, highlighting the concept of this type of crime, relevant and specific legislation and forms of preventive investigation used by the police. Then, through such a breach of order, the phase of consubstantiation of the illicitness occurred occurs, and it is at this point that the main occurrence of this study occurs, making computational forensic expertise as an exclusive science for obtaining criminal indications within the virtual environment for confection Of verifying reports. In addition, within this niche, as a specification of the proposed theme, some tools are highlighted aimed at capturing the data guiding the investigation and expertise of virtual crimes occurred within computer networks.

Keywords: Computer networks; Information security; Virtual crime; Computational forensic expertise

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA – Advanced Research Project Agency

ARPANET – Advanced Research Projects Agency Network

BDTD – Biblioteca Digital Brasileira de Testes e Dissertações

CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CERN – Conselho Europeu para a Pesquisa Nuclear em Genebra

CD – Compact Disc

CP – Código Penal

DAT – Digital Audio Tape

DeMa – Decode Manager

DLL – Dynamic-Link Library

DVD – Digital Versatile Disc

DNS – Domain Name System

EC – Estória Cobertura

E-MAIL – Eletronic Mail

FTP – File Transport Protocol

HD – Hard Disk

HTML – Hyper Text Markup Language

HTTP – Hyper Text Transfer Protocol

IMAP – Internet Message Access Protocol

IP – Internet Protocol

IPV4 – Internet Protocol version 4

IPV6 – Internet Protocol version 6

MFT – Master File Table

MILNET – Military Network

MP – Módulos Processadores

PC – Personal Computer

PCAP – Packet Capture Data Format

PHP – Personal Home Page

PIPI – Porta Independente Protocolo de Identificação

POP – Post Office Protocol

RTP – Real-time Transport Protocol

SENASP – Secretaria Nacional de Segurança Pública

SIP – Session Initiation Protocol

SMTP – Simple Mail Transfer Protocol

TCP – Transport Control Protocol

UCE – Unsolicited Commercial E-mail

UDP – User Datagram Protocol

VOIP – Voice Over IP

TFTP – Trivial File Transfer Protocol

TI – Tecnologia da Informação

WWW – World Wide Web

SUMÁRIO

INTRODUÇÃO

A segurança pública é o método de proteção e garantidora dos direitos individuais da pessoa humana, assegurando o pleno exercício da cidadania. Nessa lógica, estando profundamente ligada a qualidade de vida dos cidadãos, a segurança pública é condição de extrema relevância para o exercício da liberdade humana. Diante desse aspecto, ações preventivas e repressivas por parte do estado tornam-se indispensáveis, principalmente no que refere às ações criminosas. No entanto, observa-se que segurança pública, conforme a constituição brasileira, é também de responsabilidade de todos (SANTOS, 2006).

Atualmente está perceptível o aumento exponencial de crimes de toda ordem que atentam contra os direitos dos cidadãos e a segurança pública, dentre esses e sendo objeto de estudo deste trabalho, encontra-se o crime virtual.

Com o advento da internet e o crescimento das tecnologias de informação e comunicação, tal modalidade de crime tornou-se amplamente utilizada por criminosos que, aproveitando da baixa exposição e as facilidades que esses sistemas de comunicação proporcionam, praticam atos ilícitos de toda natureza (FERREIRA, [2009]).

A simplicidade de interação nos meios de comunicação oportunizando realizações de transações bancárias, consultas de qualquer tipo de informação e troca de mensagens com o mundo todo, atraiu a ação de criminosos que viram na internet possibilidades infinitas de fraudar e roubar informações utilizando de muitos meios fraudulentos para a prática de crimes dentro do mundo virtual (SÔNEGO, 2012).

O crime virtual, de acordo com Rossini (2004, p. 110 apud PINHEIRO, [2006?], p. 15) define-se,

> [...] pela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Por terem características de execução diferentes do crime comum, há a necessidade de um tratamento diferenciado em relação à obtenção de provas para seu esclarecimento. Essa diferenciação ocorre devido ao cenário do crime ser em parte ou no todo virtual. Nesse ponto, há a necessidade de realização de uma perícia específica que analise as provas no ambiente computacional, a fim de direcionar decisões importantes para a aplicação das sanções devidas.

Dessa maneira, a perícia forense computacional, de acordo com Eleutério e Machado (2011, p. 31 apud GONÇALVES et al, 2012, p. 2, 3) "[...] é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo". Possuindo então, a capacidade de envolver a polícia dentro de um trabalho investigativo e pericial na resolução de crimes cometidos pelo uso do computador (ELEUTÉRIO; MACHADO, 2011 apud GONÇALVES et al, 2012).

Contudo, há de se salientar que métodos de proteção e prevenção ao crime virtual existem. E é nesse ponto que se torna fundamental que se considere aspectos relacionados à segurança da informação, haja vista que, essa é a área específica no universo tecnológico que expõe conceitos e tratamentos da informação relativos a segurança em qualquer instância em que dados ou informação estiverem inseridos.

Levando em consideração esses aspectos, Fontes (2006) assevera que a informação é algo muito valioso necessitando de proteção, e que certas políticas relacionadas a sua segurança devem ser tratadas com muita atenção, de forma a evitar as ameaças que se encontram, principalmente, nos sistemas de comunicação.

As formas de proteção da informação têm que estar inseridas no cotidiano dos usuários de qualquer sistema informático de comunicação e processamento de dados, pois um sistema pode estar exposto a muitos tipos de ameaças, que sem uma proteção devida causam danos, muitas vezes irreparáveis, às informações (SOARES; LEMOS; COLCHER, 1995). Muitos tipos de vírus e ataques estão por toda internet a fim de prejudicar pessoas, sistemas ou organizações e beneficiar criminosos. Recursos fundamentais que garantam a

confidencialidade, integridade e disponibilidade da informação são itens de extrema importância à sustentação da segurança de dados e informação (BEAL, 2005), e quem preza pela sua integridade e pela idoneidade de seus dados e informações tem que estar alerta a esses fundamentos.

Diante dessa perspectiva, busca-se formas de minimizar as ações criminosas relacionadas ao mundo virtual aplicando conhecimentos e técnicas em diversas áreas buscando subsídios fornecedores de garantias para a aplicação de sanções em quaisquer esferas. Sendo para isso necessária uma investigação pontual e substancial, levando-se em conta sempre o apoio das tecnologias disponíveis.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Apresentar um estudo sobre softwares forenses capazes de capturar vestígios nos casos de crime virtual ocorrido em rede de computadores.

1.1.2 Objetivo específico

- Caracterizar redes de computadores mencionando elementos responsáveis pela segurança da informação;
- Conceituar e identificar os tipos de crime virtual apresentando a legislação específica vigente;
- Identificar conceitos, procedimentos e técnicas envolvidas com a perícia forense computacional e modelos de investigação policial;
- Apresentar softwares que apontam vestígios para investigação forense em redes de computadores.

1.2 PROBLEMÁTICA

- O que é crime virtual e qual o método utilizado para investigação desses crimes?

- Existem formas de prevenção ao crime virtual?
- Quais as ferramentas que auxiliam a investigação em crimes virtuais nas redes de computadores?

1.3 JUSTIFICATIVA

Com o surgimento e estabelecimento da internet e a popularização das redes de computadores dentro do cotidiano da sociedade, a segurança de informação tem sido colocada em evidência, explicitando a ocorrência de crimes virtuais bem como maneiras de evitá-los ou mesmo minimizá-los. Esses crimes motivados pela baixa exposição do criminoso gerando a "falsa" sensação de anonimato ou pelo criminoso ver a internet como um campo farto de vítimas descuidadas com a segurança podendo obter muitas vantagens sem a utilização de meios violentos na sua ação, tornaram-se muito frequentes e aumentaram exponencialmente.

Diante deste panorama, percebe-se a relevância da ação de uma perícia exclusiva e pontual para a indicação de indícios que apontem o direcionamento da investigação e processo penal. Nesse ponto, a perícia forense computacional torna-se fundamental para a investigação dos crimes virtuais.

Sendo assim, com a intenção de construir e evidenciar conhecimentos que atuam na área da perícia forense computacional na investigação do crime virtual, trazendo conceitos de segurança da informação dentro e fora da rede de computadores, tem-se a construção deste estudo a fim de produzir e evidenciar conhecimentos nas áreas supracitadas, levando à sociedade a compreensão do que circunda o crime virtual e sua forma de investigação bem como modos de se proteger, viabilizando maior percepção de áreas de conhecimento pouco difundidas no cotidiano.

1.4 PROCEDIMENTOS METODOLÓGICOS

A metodologia utilizada tem por base uma pesquisa teórica de cunho qualitativo tendo por finalidade, de início, identificar tipos de redes de computadores expondo o funcionamento do grupo de protocolos de comunicação TCP/IP (*Transport Control Protocol/Internet Protocol*) que é o responsável por unir redes distintas evidenciando a *internet* como o principal meio virtual. Nessa temática ainda agrega-se formas de segurar à

rede de computadores e aos envolvidos no processo de comunicação conceitos sobre a segurança da informação trazendo métodos essenciais para a proteção da informação dentro e fora da rede de computadores. Será relacionado, ainda, os perigos escondidos dentro do mundo virtual explicitando os diversos modos e técnicas envolvidas na captura da informação para realização das mais variadas fraudes.

Posteriormente é tratado do crime virtual, de forma a conceituá-lo no meio informático e criminal, caracterizando os tipos de crimes virtuais pelos seus *modus operandi*. Nesse contexto são relacionadas as leis brasileiras específicas que tratam sobre este conteúdo. E, por conseguinte, torna-se necessário evidenciar as fases da perícia forense computacional explicitando as técnicas envolvidas nessa ciência forense específica para obtenção e tratamento de evidências e os modos de investigação dos crimes virtuais na grande rede de computadores.

Por fim, como proposta geral deste estudo, é demonstrado o funcionamento de alguns *softwares* que fazem a busca por vestígios dentro da rede de computadores e trazem dados complementares para o direcionamento da investigação em crimes ocorridos em redes de computadores.

1.4.1 Revisão de literatura

Com a finalidade de conhecer o estado de desenvolvimentos dos estudos na literatura científica sobre os assuntos envolvidos dentro da temática proposta mapeando as publicações mais adequadas e os principais autores para análise da coleção obtida, foi realizado uma busca nos portais CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) e BDTD (Biblioteca Digital Brasileira de Testes e Dissertações). Para a condução da pesquisa envolvida foram abordados temas que compõem a ideia central da problemática, tais como: crime virtual, forense computacional, segurança da informação e redes de computadores.

Para a busca nos dois portais foram definidas um padrão de palavras-chaves de acordo com cada assunto, vistos a seguir:

- Crime virtual: “crime virtual”, “crime cibernético”, “cibercrime”;
- Forense computacional: “forense computacional”; “computação forense”

- Segurança da informação: “segurança informação”, “segurança informática”, “segurança cibernética”;

- Redes de computadores: “redes de computadores”, “segurança em redes de computadores”;

Cabe ressaltar que o idioma português e apenas artigos, dissertações e teses foram utilizados como refinamento padrão para todas as pesquisas. E o julgamento das pesquisas selecionáveis deu-se através da leitura dos resumos e algumas partes dos trabalhos elencando-se aquelas que demonstraram relação com o tema principal.

Na busca nos portais indicados - CAPES e BDTD - pelas palavras-chaves dos assuntos relacionados obteve-se o seguinte resultado:

- Crime virtual: 03 teses, 01 dissertação, 01 artigo;

- Forense computacional: 02 teses, 01 dissertação;

- Segurança da informação: 03 teses; 02 dissertações, 02 artigos;

- Redes de computadores: 02 teses;

Destas referências pesquisadas, a Tabela 1 elenca algumas que mais se relacionam com a temática desse trabalho:

PRINCIPAIS REFERÊNCIAS		
TÍTULO	**AUTOR**	**BASE DE DADOS**
Estudo da eficiência jurisdicional no direito cibernético. Revista Eletrônica do Ministério Público do Estado de Goiás. 2012.	Douglas Ferreira Magalhães	CAPES
A segurança do conhecimento nas práticas da gestão da segurança da informação e da	Wagner Junqueira de Araújo	CAPES

gestão. Revista Ibero-Americana de Ciência da Informação do conhecimento. 2011.		
Planejamento e implementação de um sistema de gestão da segurança da informação	Bruna Patrícia Ribeiro Alves da Silva	CAPES
Forense computacional em ambiente de rede baseado na geração de alertas de sistemas de detecção de intrusos auxiliado pela engenharia dirigida por modelos. 2012.	Lianna Mara Castro Duarte	BDTD
Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos. 2009.	Maciel Colli	BDTD

Tabela 1 – Principais referências

Diante do resultado obtido da pesquisa, percebe-se a relevância desse trabalho já que pouco se está produzindo sobre o tema principal que é demonstrar ferramentas utilizadas no direcionamento da perícia forense computacional e investigação policial. A demonstração dos assuntos envolvidos, principalmente no que toca a investigação forense através de softwares, é pouco mencionada nos trabalhos pesquisados, gerando assim, a necessidade de confecção do tema proposto. No entanto, nota-se alguns trabalhos que certamente contribuem para embasamento e confecção dos assuntos transversais deste estudo.

1.5 ORGANIZAÇÃO DA APRESENTAÇÃO

Este trabalho está organizado da seguinte forma:

O capítulo 2 apresenta a definição de redes de computadores trazendo aspectos relacionados ao modelo de referência TCP/IP e o surgimento da internet relacionando com procedimentos envolvidos no processo da segurança da informação.

No capítulo 3 são mencionados os conceitos sobre crime virtual trazendo os tipos, os métodos de investigação e a legislação vigente envolvidos nesse tipo de crime.

O capítulo 4 são evidenciadas ferramentas específicas da perícia forense computacional utilizadas em casos de crimes ocorridos por meio da rede de computadores.

Por fim, no capítulo 5 são apresentadas as considerações finais e recomendações para trabalhos futuros.

2. REDES DE COMPUTADORES E A PROTEÇÃO DA INFORMAÇÃO

As redes de computadores estão inseridas em todo ambiente em que haja comunicação de dados. E a garantia de tráfego desses dados têm que obedecer a alguns requisitos, principalmente no tocante à segurança da informação. Este capítulo tem por objetivo conceituar redes de computadores caracterizando a internet como a principal rede no mundo capaz de conectar as pessoas no ambiente virtual correlacionando os atributos característicos da segurança da informação dentro e fora da rede de computadores.

2.1 REDES DE COMPUTADORES

A comunicação sempre foi uma das maiores necessidades da humanidade. No decorrer do tempo, com esta necessidade aumentando devido ao grande crescimento da sociedade e de sua dispersão geográfica, tornaram-se imprescindíveis maneiras de efetuar algum tipo de comunicação com comunidades distantes. Pombos-correios e sinais de fumaça foram usados pelos ancestrais do homem para a comunicação e, posteriormente, a invenção do telégrafo em 1838 deu entrada a uma nova época nas comunicações (SOARES; LEMOS; COLCHER, 1995).

A evolução na área da comunicação, processamento e armazenamento das informações possibilitou uma revolução de novas formas de comunicação, permitindo maior eficácia dos sistemas computacionais. Em seguida, com a evolução dos sistemas de computação e das arquiteturas, surgem as redes de computadores como uma forma mais eficaz de comunicação (SOARES; LEMOS; COLCHER, 1995).

Tanenbaum (1997) define redes de computadores como computadores autônomos interconectados, onde estes realizam a troca de informações. O autor ainda complementa evidenciando que, para que computadores sejam considerados autônomos, torna-se imprescindível não haver uma relação mestre/escravo entre eles. Ou seja, um sistema onde um computador pode iniciar, encerrar ou controlar outro computador não é considerado uma rede, pois não há caracterização alguma de autonomia.

De uma forma muito semelhante, Soares, Lemos e Colcher (1995, p.10) caracterizam rede de computadores como um "[...] conjunto de módulos processadores (MPs) capazes de trocar informações e compartilhar recursos, interligados por um sistema de comunicação [...]". Os autores ainda referem-se a MP como "[...] qualquer dispositivo capaz de se comunicar através do sistema de comunicação por troca de mensagens" (SOARES; LEMOS; COLCHER, 1995, p.10). Logo, sistema de comunicação constitui-se de MPs ligados aos meios de comunicação organizados por protocolos dentro de um arranjo topológico (SOARES; LEMOS; COLCHER, 1995).

Hayden (1999 p. 4) afirma que uma rede de computadores deve possuir regras básicas para a garantia do envio seguro das informações:

- As informações devem ser enviadas de maneira segura, sem qualquer dano nos dados.
- As informações devem ser enviadas de maneira coerente – a rede deve ser capaz de determinar para onde as informações estão indo.
- Os diversos computadores devem ser capazes de identificar uns aos outros dentro da rede.
- Deve haver uma maneira padronizada de nomear e identificar as partes que compõem a rede.

Nota-se a concordância dos autores sobre a definição de redes de computadores consentindo que, uma rede de computadores está ligada à troca de informações entre os hosts conectados. Doravante, torna-se necessário explicitar a forma como se deu o início da *internet* (a grande rede mundial de computadores) através da conexão de redes distintas.

2.2 O CONJUNTO DE PROTOCOLOS TCP/IP E A INTERNET

Para o surgimento da *internet* como é conhecida atualmente, alguns caminhos tiveram que ser percorridos para a possibilidade dessa junção e entrelaço dos computadores

espalhados pelo mundo. Por esse motivo, será tratado nesse momento sobre o surgimento da *internet* e, a necessidade da confecção de um conjunto de protocolos utilizados para o aperfeiçoamento da *internet:* o conjunto de protocolos TCP/IP.

A história começa em 1960 com a necessidade do Departamento de Defesa Americano de projetar uma rede militar de comunicação onde, mesmo sob um ataque a uma parte dessa rede, fosse possível ainda realizar a troca de informações entre as estações. Nesse intuito, o pesquisador Paul Baran concebeu um conjunto que teria como base um sistema descentralizado. Esse conjunto baseava-se em uma rede tecida como uma teia de aranha onde os dados percorreriam os melhores caminhos possíveis a fim de chegar ao destino esperado (DUMAS, 2013).

Em 1969 nascia, então, a ARPANET (*Advanced Research Project Agency Network*), oriunda das pesquisas realizadas pela *Advanced Research Project Agency* (ARPA), um órgão ligado ao Departamento de Defesa Americano. Posteriormente, a parte de comunicação militar da rede foi dividida tornando-se a MILNET (*Military Network*) deixando para uso civil a ARPANET (DUMAS, 2013).

“Pouco a pouco, centenas de universidades e repartições públicas foram conectadas, usando linhas telefônicas dedicadas” (TANENBAUM, 2003, p. 44). Contudo, após a criação de redes de rádio e satélite, começaram a surgir problemas com os protocolos existentes, o que levaria à criação de uma arquitetura de referência padrão para a conexão de redes distintas de maneira uniforme (TANENBAUM, 2003). “Mais tarde essa arquitetura ficou conhecida como Modelo de Referência TCP/IP, graças a seus dois principais protocolos” (TANENBAUM, 2003, p. 44).

Uma etapa decisiva foi superada em 1990 com a criação, por um pesquisador do Conselho Europeu para a Pesquisa Nuclear em Genebra (Cern), Tim Berners-Lee, do protocolo HTTP (*Hyper Text Transfer Protocol*) e da linguagem HTML (*Hyper Text Markup Language*), que permitiram navegar de um site a outro, ou de uma página a outra. A *World Wide Web* (WWW) lançou seu voo, e a internet se abriu ao público, empresas particulares e privadas. Uma multidão de sites apareceu (DUMAS, 2013).

A arquitetura Internet TCP/IP é organizada em quatro camadas conceituais conforme Soares, Lemos e Colcher (1995):

- Camada de aplicação;
- Camada de transporte;
- Camada de inter-rede;
- Camada de interface de rede.

A Figura 1 a seguir destaca o modelo TCP/IP:

Figura 1: Modelo TCP/IP

Fonte: APARÍCIO (2012).

No nível de aplicação, os usuários usam aplicações para ter o acesso aos serviços da camada de inter rede. Essas aplicações interagem com a camada de transporte no envio e no recebimento de dados utilizando-se dos protocolos TCP e UDP (*User Datagram Protocol*), presentes na camada de transporte (SOARES; LEMOS; COLCHER, 1995). Esta camada "[...] possui todos os protocolos de nível mais alto. Dentre eles estão o protocolo de terminal virtual (TELNET), o protocolo de transferência de arquivos (FTP – *File Transport Protocol*) e o protocolo de correio eletrônico (SMTP - *Simple Mail Transfer Protocol*)" (TANENBAUM, 2003, p. 46, 47). Logo em seguida foram adicionados outros protocolos como o DNS *(Domain Name System*) que mapeia os nomes de hosts para seus respectivos endereços de rede e o HTTP que é usado para buscar páginas na *World Wide Web* (TANENBAUM, 2003).

Abaixo da camada de aplicação encontra-se a camada de transporte. Esta camada é responsável por permitir a conversação da origem ao destino entre as aplicações. É nessa camada que se encontra o protocolo TCP que realiza serviços orientados à conexão fornecendo controle de erro, controle de fluxo, sequenciação e multiplexação do acesso ao nível inter rede e ao UDP que, fornecendo um serviço não orientado à conexão e sendo um

protocolo mais simples, realiza multiplexação/demultiplexação do acesso ao nível inter-rede (SOARES; LEMOS; COLCHER, 1995).

Conforme Tanenbaum (2003, p. 45) a camada inter redes tem a função de "[...] permitir que os hosts injetem pacotes em qualquer rede e garantir que eles trafegarão independentemente até o destino (talvez em uma rede diferente)". O autor ainda comenta que os pacotes podem chegar em uma ordem diferente daquela em que foram enviados, tornando responsabilidade das camadas superiores a reorganização (TANENBAUM, 2003).

> A camada inter redes define um formato de pacote oficial e um protocolo chamado IP (*Internet Protocol*). A tarefa da camada inter redes é entregar pacotes IP onde eles são necessários. O roteamento de pacotes é uma questão de grande importância nessa camada, assim como a necessidade de evitar o congestionamento. (TANENBAUM, 2003, p. 45)

A camada de interface de rede é responsável pela compatibilização das redes que se ligam à inter rede. Ela permite que qualquer tipo de rede possa se conectar desde que essa rede possua uma interface que compatibilize a sua tecnologia específica com o protocolo IP. Em seguida, o nível de interface de rede recebe os datagramas IP do nível de inter rede e transmite através de uma rede específica traduzindo os IPs para os endereços físicos dos hosts ou gateways conectados à rede (SOARES; LEMOS; COLCHER, 1995).

Contudo, torna-se essencial que elementos que proporcionem segurança à informação sejam avaliados de forma que, garantam alguns princípios ao bom tráfego de dados e informações na *internet*. Diante desse aspecto, o capítulo seguinte mencionará elementos destinados a garantir a segurança da informação.

2.3 SEGURANÇA DA INFORMAÇÃO

Em início, torna-se necessário a definição do que é informação e qual a sua importância no mundo. Nesse sentido, Sônego (2012, p. 11) classifica a informação como "[...] o resultado do processamento, manipulação e organização de dados de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe". E Beal (2005) complementa que a informação, pela sua alta capacidade de adicionar valor a processos, produtos e serviços, possui caráter cada vez mais crítico para a realização dos objetivos organizacionais.

A informação é um ativo muito valioso para uma organização e precisa ser protegida contra qualquer fator que traga ameaças à sua integridade. É nesse âmbito que a segurança da informação entra para proteger os ativos valiosos de informação que se encontram dentro de componentes de TI (Tecnologia da Informação) e também naquelas que se encontram armazenadas na mente humana, num pedaço de papel ou em microfichas e microfilmes, tendo em vista que, estas informações são também de extrema relevância (BEAL, 2005).

Fontes (2006, p. 2) afirma que a "informação é muito mais que um conjunto de dados". A informação é algo muito precioso para um indivíduo ou organização, e quando principalmente se trata de uma organização fica evidente a necessidade de métodos de proteção a este bem valioso. Uma organização deve possuir regulamentos (políticas, normas e regras) de segurança de informação para evitar que o negócio seja prejudicado pelo mau uso da informação. Estes regulamentos imprescindivelmente necessitam estar explícitos para todos os usuários que acessam e usam a informação, de forma a evitar perdas, danos, destruição e/ou mau uso (FONTES, 2006).

Kolling ([2010]a) comenta que a segurança da informação refere-se à proteção de dados relevantes a uma organização ou a um indivíduo. Sendo informação todo o conteúdo ou dado que contém um valor que servirá a determinados propósitos de utilidade do ser humano.

Atualmente, a informação digital tornou-se fundamental necessitando de aparatos que garantam cada vez mais a proteção. A segurança dessas informações pode ser afetada por diversos fatores, como os comportamentais do usuário, a infraestrutura onde se encontram as informações e por pessoas que objetivam roubar, destruir ou modificar essas informações (KOLLING, [2010]a).

Beal (2005, p. 1) refere que "Segurança da informação pode ser entendida como o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade".

Da mesma forma Beal (2005) e Kolling ([2010]a), enumeram como os três objetivos fundamentais na preservação da informação: a confidencialidade, integridade e disponibilidade.

Segundo Beal (2005):

- **Confidencialidade:** o acesso às informações é garantido e restrito a usuários legítimos;
- **Integridade**: garante que as informações não sejam alteradas ou excluídas sem autorização. Consiste em prevenir contra a criação, alteração ou destruição não autorizada garantindo que as informações permaneçam completas e precisas;
- **Disponibilidade:** garante que a informação seja disponibilizada apenas para os usuários legítimos.

Outros objetivos ainda são acrescidos a esses três, o de legalidade e o de uso legítimo (BEAL, 2005). O de legalidade garante "[...] que a informação foi produzida em conformidade com a lei [...]" (BEAL, 2005, p. 1). E de uso legítimo garante "[...] que os recursos de informação não são usados por pessoas não autorizadas ou de maneira não autorizada" (BEAL, 2005, p. 1).

Agregando ainda a estes objetivos fundamentais à proteção da informação, Fontes (2006) acrescenta a auditabilidade e o não repúdio de autoria. O autor discorre conceituando a auditabilidade como forma de garantir que o acesso e o uso da informação sejam registrados, possibilitando assim, a identificação de quem realizou o acesso e qual a modificação que este promoveu. No que se refere ao não repúdio de autoria, o autor descreve que "[...] o usuário que gerou ou alterou a informação (arquivo de texto ou mensagens de correio eletrônico) não pode negar o fato, pois existem mecanismos que garantem sua autoria" (FONTES, 2006, p. 12).

Quando a informação necessita ser transmitida num processo de comunicação, outros fatores além dos apresentados precisam ser levados em consideração. Tais fatores visam evitar fraudulências de documentos em trânsito e disputas sobre a origem de uma comunicação ou o recebimento de uma informação transmitida (BEAL, 2005).

Conforme Beal (2005, p. 2) "A segurança da comunicação visa proteger a informação que trafega de um ponto a outro, com o objetivo de preservar: "

- **Integridade do conteúdo:** garantia de que a mensagem enviada pelo emissor é recebida de forma completa e exata pelo receptor.
- **Irretratabilidade da comunicação:** garantia de que o emissor ou receptor não tenha como alegar que uma comunicação bem-sucedida não ocorreu.
- **Autenticidade do emissor e do receptor:** garantia de que quem se apresenta como remetente ou destinatário da informação é realmente quem diz ser.

> - **Confidencialidade do conteúdo:** garantia de que o conteúdo da mensagem somente é acessível a seu(s) destinatário(s).
> - **Capacidade de recuperação do conteúdo pelo receptor:** garantia de que o conteúdo transmitido pode ser recuperado sem sua forma original pelo destinatário. Para que esse objetivo seja alcançado, emissor e receptor precisam usar protocolos de comunicação consistentes [...]. (BEAL, 2005, p. 2)

2.3.1 Ameaças à Segurança da Informação

Um sistema pode estar exposto a muitos tipos de ameaças. E tais ameaças podem causar todo tipo de violação em um sistema ocasionando, principalmente, grandes danos às informações. Em vista disso, torna-se muito importante a necessidade de proteção contra a manipulação, intencional ou não, das informações confidenciais e dos dispositivos periféricos do computador por elementos não autorizados (SOARES; LEMOS; COLCHER, 1995).

Soares, Lemos e Colcher (1995) arrolam algumas possíveis ameaças a redes de computadores:

- Destruição de informação ou de outros recursos.
- Modificação ou deturpação da informação.
- Roubo, remoção ou perda de informação ou de outros recursos.
- Revelação de informação.
- Interrupção de serviços.

As ameaças podem ocorrer a qualquer momento e se aproveitam das falhas de segurança da organização causando danos, perdas e prejuízos. As ameaças podem ser naturais, ou seja, decorrentes da natureza, tais como, fogo, enchentes, terremotos que podem causar dano aos ativos de informação. Contudo, existem as ameaças intencionais e involuntárias (NASCIMENTO, 2013).

As ameaças involuntárias são ocasionadas por descuidos, desconhecimentos e erros no trato para com o ativo de informação, seja por falta de treinamento de funcionários, infecção por vírus ou acessos indevidos. Diferentemente das ameaças intencionais que são provocadas por invasões, fraude e roubos de informações (NASCIMENTO, 2013).

Soares, Lemos e Colcher (1995) complementam mencionando que as ameaças ainda podem assumir o papel de passivas e ativas. Sendo passiva aquela que não resulta em

qualquer alteração nas informações. Tendo como exemplo “Uma estação que processa todos os quadros que recebe em uma rede local (incluindo os que não são a ela endereçados) ” (SOARES; LEMOS; COLCHER, 1995, p. 448).

No entanto, de maneira oposta, uma ameaça ativa é configurada por realizar modificações nas informações contidas no sistema ou modificações em seu estado de operação (SOARES; LEMOS; COLCHER, 1995). Como exemplo tem-se “Uma estação de uma rede em anel que não transmite mensagens quando deveria fazê-lo (ela não é a responsável pela retirada da mensagem do anel) [...]” (SOARES; LEMOS; COLCHER, 1995, p. 448, 449).

A seguir, estão relacionados alguns exemplos de possíveis ameaças à segurança da informação principalmente no ambiente digital:

- **Vírus:** programa com fins maliciosos que tem a capacidade de apagar ou alterar arquivos de usuários, prejudicar o funcionamento do sistema operacional, causar excesso de tráfego na rede, entre outros males (ALECRIM, 2011).

Kolling ([2010]b) comenta que existem vários tipos de vírus, alguns deles são:

> - **Vírus de Macro**: São vírus feitos na linguagem dos macros e funcionam dentro dos programas em que estão interligados. Ou seja, ao abrir um arquivo de *Power Point* (.ppt) infectado com esse tipo de vírus, por exemplo, o vírus é automaticamente ativado e grava arquivos que substituem partes dos comandos normais do programa.
> - **Vírus de Boot**: É o tipo de vírus mais comum. Para infectar a máquina com ele, basta colocar um disquete infectado no drive.
> - **Vírus de Arquivo**: São os vírus que ficam 'guardados' em arquivos executáveis, que geralmente são de extensão EXE ou COM. Esse tipo de vírus altera o arquivo original e o leva até a memória RAM (*Random Access Memory*) antes do arquivo original e correto. A partir do momento que ele chega à memória, acaba contaminando todos os outros arquivos executáveis.
> - **Vírus de Programa**: Assim como os vírus de arquivos, infectam arquivos executáveis e podem impedir o usuário até de ligar a máquina.
> - **Cavalos de Tróia**: É um tipo de vírus que permite total acesso remoto à máquina após a infecção. Pode também ter outras funções como roubar dados do usuário e executar instruções de scripts. Entre essas instruções, podem surgir ordens de deletação de arquivos, destruição de aplicativos, etc.
>
> A partir do momento em que um cavado de tróia permite o acesso à uma máquina, ele passa a utilizar portas TCP e acaba alertando ao seu criador que aquele computador está 'disponível'.

- ***Keylogger*:** aplicativo que captura tudo que o usuário digita. É muito usado para conseguir

senhas de acesso a contas e, geralmente está embutido em vírus, *spywares* ou *softwares* de procedência duvidosa (ALECRIM, 2011).

- ***Backdoor:*** é uma falha de segurança, conhecida como porta dos fundos, onde um programa ou sistema operacional permite a invasão de um *cracker* no sistema, que obtém acesso total da máquina, podendo instalar vírus e programas maliciosos (KOLLING, [2010]b).
- ***Spam*****:** é um *e-mail* (*electronic mail*) indesejado não solicitado pelo usuário e que, geralmente é despachado para muitas pessoas. Pode conter vírus agressivos que capturam informações pessoais, mas na maioria das vezes os *e-mails* aparecem como propagandas. Também são chamados de UCE (*Unsolicited Commercial E-mail*) (GUERRA, 2012).
- ***Phishing*****:** é a fraude que ocorre através do envio de mensagens não solicitadas. Estas mensagens levam o usuário a acessar páginas falsas pensando ser de uma empresa, banco, ou organizações conhecidas. Ao acessar a página, o usuário tem seus dados pessoais e/ou financeiros capturados (KOLLING, [2010]b).
- ***Worm*****:** programa semelhante ao vírus, no entanto ele cria cópias de si mesmo podendo infectar outros computadores. A infecção pode ocorrer através de redes locais, rede social, *e-mails, internet* (MARTINS, 2008).
- **Negação de serviço:** é conhecido como **DoS** (*Denial of Service*), este ataque consiste em um usuário mal intencionado usar de um computador para tirar outro de operação negando-lhe acesso à internet ou serviço (KOLLING, [2010]b).
- **Engenharia social:** é a habilidade de conseguir acesso a informações confidenciais utilizando habilidades de persuasão. Neste modelo de ameaça o fator humano é o alvo devido à falta de percepção das pessoas em relação à importância das informações que elas detêm (CIPOLI, 2012).
- ***Adware e spyware*****:** Os *adwares* têm a função de projetar propagandas através de um browser ou programa instalado no computador de forma muitas vezes invasivas e perigosas, podendo minar as configurações de segurança para rastrear suas atividades. De maneira semelhante, os *spywares* captam informações como dados do usuário e repassam para terceiros, sem autorização (KOLLING, [2010]b).

2.3.2 Mecanismos de proteção

Uma política de segurança deve ser implementada utilizando-se de vários mecanismos de controle de segurança com a finalidade de se obter a maior proteção possível dentro dos parâmetros levantados. Nesse contexto, observa-se uma vasta gama de controles aplicáveis à segurança da informação, pois é substancial que se avalie três fatores reais: a segurança física, tecnológica e humana (SÊMOLA, 2003).

Fontes (2006, p. 58) frisa que "toda a informação deve ser protegida contra desastres físicos (fogo, calor, inundações, entre outros) e lógicos (vírus, acesso indevido, erro de programas, alteração incorreta, entre outros) ".

Em relação ao recurso humano, dentro de qualquer esquema de segurança da informação, é notável que estes se tornem o elo mais frágil. Pois, por mais sofisticado que seja o esquema de segurança de uma organização ele pode ser facilmente quebrado por privilégios de acesso de usuários mal intencionados ou despreparados (BEAL, 2005).

Beal (2005) indica que grande parte dos incidentes de segurança são ocasionados por integrantes da própria organização, sendo uma pequena parcela destinada aos ataques por hackers. Dentre os incidentes, estão aqueles "[...] acidentais (decorrentes de ignorância, erro, negligência ou distração) ou intencionais (por motivos de fraude, vingança, descontentamento etc.)" (BEAL, 2005, p. 71).

Sêmola (2003) lista alguns itens para a redução de riscos relacionados ao capital humano:

- Seminários de sensibilização;
- Cursos de capacitação;
- Campanhas de divulgação da política de segurança;
- Crachás de identificação
- Procedimentos específicos para demissão de admissão de funcionários;
- Procedimentos específicos para tratamento de recursos terceirizados;
- Termo de responsabilidade;
- Termo de confidencialidade;
- Softwares de auditoria de acessos;

- Softwares de monitoramento e filtragem de conteúdo;

"Quando a organização define uma política de segurança, seu objetivo é explicitar aos usuários que acessam e utilizam qual é a filosofia e quais são as regras sobre esse recurso" (FONTES, 2006, p. 73).

Beal (2005) frisa que um aspecto muito importante na segurança da informação é a proteção contra os ataques de engenharia social. Devido aos hackers e outras pessoas mal-intencionadas usarem de sua persuasão para obter dados e informações valiosas de usuários ingênuos, ignorantes ou mal treinados, tornam-se necessários programas de treinamentos que visam conscientizar todo o recurso humano da organização sobre a importância de se manter em sigilo informações pessoais e confidencias.

Sêmola (2003) também apresenta alguns elementos relativos à segurança física voltados a controlar o acesso e as condições de ambientes físicos, sinalizando, registrando, impedindo e autorizando acessos e estados, são eles:

- Roletas de controle de acesso físico;
- Climatizadores de ambiente;
- Detectores de fumaça;
- Acionadores de agua para combate a incêndio;
- Extintores de incêndio;
- Cabeamento estruturado;
- Salas-cofre;
- Dispositivos de biometria;
- *Smartcards*;
- Certificados digitais em Token;
- Circuitos internos de televisão;
- Alarmes e sirenes;
- Dispositivos de proteção física de equipamentos
- *Nobreaks*;

- Dispositivos de armazenamento de mídia magnética;
- Fragmentadores de papel;
- Entre outros.

E sobre a segurança tecnológica em um ambiente de comunicação de dados evidenciam-se alguns recursos:

- **Autenticação:** este método é utilizado para gerenciar o acesso aos recursos do sistema. Estabelece identificadores e senhas para esta estipular categorias de usuários, de forma a limitar os acessos (BEAL, 2005);
- ***Firewall*:** "[...] barreira de proteção que controla o tráfego de dados do computador e da internet. O objetivo desse dispositivo é permitir somente a transmissão e recepção de dados autorizados e confiáveis" (KOLLING, [2010]c). Este dispositivo pode assumir a forma de um software e também de um hardware especializado, realizando análises do fluxo de pacotes de dados, filtragens e registros (SÊMOLA, 2003).
- **Detector de intrusos:** conhecido como IDS (*Intrusion Detection Systems*) "[...] é um dispositivo complementar ao firewall que agrega mais inteligência ao processo de combate a ataques e invasões" (SÊMOLA, 2003, p. 121). Diferencia-se do firewall por ser orientado por uma base de dados que contêm informações sobre comportamentos suspeitos de pacotes de dados e assinaturas de ataques (SÊMOLA, 2003).
- **Criptografia:** "Com certeza, a ferramenta automatizada mais importante para a segurança de rede e das comunicações é a criptografia" (STALLINGS, 2008, p. 15). Burnett e Paine (2002, p.11) descrevem que "a criptografia converte dados legíveis em algo sem sentido, com a capacidade de recuperar os dados originais a partir desses dados sem sentido". De acordo com Kolling ([2010]d), existem basicamente dois tipos de chaves criptográficas: chave simétrica e assimétrica. Na criptografia de chave simétrica é utilizada uma chave simples para codificar e decodificar a mensagem. Por outro lado, a criptografia de chave assimétrica utiliza dois tipos de chaves, a chave pública e privada. "Elas se resumem da seguinte forma: a chave pública para codificar e a chave privada para decodificar, levando-se em consideração que a chave privada é secreta" (KOLLING, [2010]d).
- ***Virtual Private Network*:** "[...] é uma forma de conectar dois computadores utilizando uma rede pública, como a internet" (MARTINS, 2009). A tecnologia de VPN (*Virtual Private*

Network) geralmente é usada por grandes empresas que possuem filiais e que necessitam interligar as duas. Para haver total segurança, esta tecnologia faz o uso do protocolo de tunelamento, que consiste basicamente em um canal principal onde há uma entrada e uma saída de informação sem que o usuário externo a esse canal possa ter acesso às informações transmitidas (MARTINS, 2009).

- ***Public Key Infrastruture*:** Segundo Carvalho (2008) "[...] é um sistema que utiliza mecanismos de segurança baseados na criptografia de chaves públicas para promover a autenticação, a confidencialidade, a integridade e o não repúdio de informações". Sêmola (2003) complementa fazendo uma analogia entre a PKI (*Public Key Infrastruture*) e um cartório tradicional, em que na hora de concretizar uma transação é necessária uma série de autenticações que comprovam a autenticidade das partes envolvidas na transação.

- **Esteganografia:** "Trata-se do estudo de técnicas que permitam esconder informações dentro de outros arquivos, sejam imagens, músicas, vídeos ou mesmo texto" (MARTINS, 2010). O fato é que a esteganografia não pode ser detectada por qualquer usuário, o sentido da mensagem a ser realmente transmitida só poderá ser desvendado pelo usuário que realmente sabe que a mensagem verdadeira está escondida. Uma das técnicas mais frequentes da esteganografia é a de esconder em arquivos a marca de direito autoral, isso evita principalmente a distribuição da informação em massa sem que o autor seja divulgado e realmente conhecido (MARTINS, 2010).

- ***Honeypots*:** De acordo com Marcelo e Pitanga (2003) *Honeypots* é um termo inglês que significa basicamente "pote de mel" que tem como principal objetivo atrair o invasor, fazendo-o pensar que o sistema a ser invadido é falho. Thomas (2007) discursa que *Honeypots* é um sistema que pode ser personalizado de acordo com o necessário e que tem como principal função atrair e prender invasores.

- **Antivírus:** Segundo Kolling ([2010]c) "Os antivírus são programas com a finalidade de detectar, prevenir e eliminar vírus de um computador". A todo o momento os usuários estão expostos aos riscos da internet, uma máquina desprotegida se torna alvo muito fácil para um *malware*, trojan ou qualquer tipo de vírus existente no mundo digital. Para assegurar total integridade da máquina faz-se necessária a inserção de um antivírus completo e estável (HAMANN, 2010).

- **Certificado digital:** “[...] funcionam como uma garantia de que você está realmente seguro, através de homologações e assinaturas criptografadas” (KARASINSKI, 2009). O certificado digital serve de base para uma certificação segura e inequívoca do autor de uma mensagem enviada ou transação realizada no meio digital. Geralmente possui uma autoridade que certifica a assinatura e a associa a um par de chaves criptográficas (ITI, [S.d.]).

Após vistos os princípios e conceitos que circundam os assuntos relativos a redes de computadores e a segurança da informação, basta, neste ínterim, conceituar e relacionar os assuntos ligados à quando o crime no ambiente virtual ocorre, evidenciando os modos de investigação e a perícia forense específica e competente para tal.

3. CRIME VIRTUAL E OS MÉTODOS DE INVESTIGAÇÃO

Este capítulo tem por objetivo apresentar conceitos ligados ao crime ocorrido dentro ou por meio do ambiente virtual, bem como trazer, em princípio, o conceito geral sobre crime comum e, posteriormente apresentar algumas legislações pertinentes ao tema. Por fim, será tratado de alguns métodos utilizados pela polícia para a investigação do crime virtual, incluindo a ciência forense distinta para os casos de crimes virtuais.

3.1 O CRIME NO MUNDO VIRTUAL: CONCEITOS E NOMENCLATURAS

Dentre as referências pesquisadas, nota-se uma divergência nos termos utilizados para esclarecer os crimes praticados através do computador. Dos termos encontrados: crime virtual, crime digital, crime por computador, crime de informática, crime telemático, entre outras nomenclaturas, será adotada para esse capítulo a terminologia crime virtual.

Contudo, antes de conceituar crime virtual, observa-se a necessidade de definir, primeiramente, o significado de crime no seu conceito geral. Crime, segundo a doutrina majoritária brasileira, é todo fato típico, ilícito e culpável. Desta forma, caracteriza-se como crime toda conduta prevista no tipo penal incriminador (fato típico), conjuntamente com tudo que contrarie a lei desde que haja danos sociais (fato ilícito ou antijurídico), e a culpabilidade que se torna evidente com a presença de três itens essenciais: a imputabilidade; a potencial consciência sobre a ilicitude do fato; e a exigibilidade de conduta diversa (FERREIRA, 2008).

Após a conceituação de crime já é possível explanar um pouco mais sobre crime virtual que é um tipo específico de crime.

Com o grande aumento da utilização de sistemas computadorizados e a expansão da internet, tornou-se frequente o uso desse meio de comunicação para a aplicação de crimes

(ROSA, 2005 apud FERREIRA, [2009]). Não possuindo fronteiras para a prática desse tipo de conduta, os malfeitores podem realizar tais crimes a partir da comodidade de seu lar, bastando apenas que tenham conhecimento e os equipamentos necessários. Essa conduta torna-se atrativa devido ao baixo risco de exposição dos criminosos (FERREIRA, [2009]). Stair e Reynolds (2006, p. 566) comentam que o crime virtual "[...] frequentemente desafia a detecção", haja vista que "[...] o crime é 'limpo' e sem violência".

E como definição, Rocha (2003 p. 188) afirma que o crime virtual "[...] consiste no fato de provocar num sistema informatizado, por meios compatíveis com ele, transferências infinitesimais e virtuais de sinais ou dados, em proveito próprio ou alheio, causando danos ou prejuízos a outrem".

De modo mais amplo, seguindo o raciocínio de Shipley e Bowker (2014), crime virtual é toda a ofensa criminal que tenha sido criada ou tornada possível pelo advento da tecnologia ou pelo crime tradicional que tem seu modo de execução modificado pelo uso da tecnologia. E, em síntese, o autor refere-se ao crime virtual como sendo o crime cometido ou facilitado através do uso da internet (SHIPLEY; BOWKER, 2014).

Do aspecto criminal, Costa (1995) define como crime virtual "[...] toda a ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão". Segundo o mesmo autor, a ação típica corresponde ao comportamento humano previsto em lei como crime, sendo que nos crimes relacionados à informática esta ação se concretiza no momento em que a utilização de um sistema de informática afeta um bem ou interesse juridicamente protegido.

Outros autores ainda agregam outros atributos ao conceito de crime virtual. Para Ramalho Terceiro (2002):

> [...] os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

E de acordo com Rossini (2004, p. 110 apud PINHEIRO, [2006?], p. 15):

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta

> típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Rosa (2005 apud FERREIRA, [2009]) destaca que existe uma diferenciação entre delito comum e delito de informática. O autor conceitua delito comum aqueles previstos na legislação brasileira dentro do Código Penal (CP) cometidos apenas com o auxílio do computador e, no que trata dos delitos de informática, esses seriam aqueles que não estão previstos no CP, porém necessitam de um computador para a obtenção do resultado desejado. Para esses crimes necessita-se de legislação específica, pois se tratam de crimes virtuais propriamente ditos.

Definindo de modo mais específico, Silva (2003, p. 60) classifica os crimes virtuais em puros, impuros e comuns. Outros autores utilizam as nomenclaturas crimes próprios para crimes puros e crimes impróprios para crimes impuros, contudo para esse assunto serão usadas as nomenclaturas de Silva (2003).

Os crimes puros "[...] referem-se aos tipos novos surgidos com o uso da informática, em que o sistema informático serve como meios e fim almejado pelo agente" (SILVA, 2003, p. 60), por outro lado, os crimes impuros "[...] são os tipos que não dependem dela, mas serve somente como meio para a prática de um delito, claramente já definido na legislação penal" (SILVA, 2003, p. 60) e, por último encontram-se os crimes comuns situados "[...] na esfera das ações, cujo sistema informático é mera ferramenta para a prática de crimes comuns, valendo ressaltar, ações já previstas como típicas em nossa legislação penal" (SILVA, 2003, p. 60).

A autora ainda menciona que alguns autores não consideram a terceira classificação mencionada, no entanto, a diferença entre esta e a segunda classificação está no fato de que, "[...] na segunda, a ação volta-se para lesionar um bem jurídico protegido pelo Direito Penal, mas que está armazenado em suporte virtual; na terceira, a ação encontra adequação típica, o meio informático é só um instrumento a mais" (SILVA, 2003, p. 60).

De um modo simples e resumido, Gomes (2000) determina a diferença entre crime puro e impuro utilizando-se dos termos crime de computador e crime no computador, respectivamente. O autor observa que "[...] no crime de computador o cibercriminoso

modifica, copia, apaga, intercepta dados, bem como invade *e-mails*, *home pages* e sistemas de rede. No caso de crime no computador, a máquina é usada apenas como *Modus Operandi*[1] do crime" (GOMES, 2000, p. 216).

3.2 LEGISLAÇÃO BRASILEIRA

Com o passar do tempo os crimes virtuais estão se tornando cada vez mais corriqueiros no Brasil. A criminalidade avança muito rapidamente e, muitas vezes, já não é possível acompanhar juridicamente as más condutas que os criminosos vêm impondo à sociedade. Diante desse motivo, gera-se lentidão no poder judiciário que acaba por não encontrar as soluções adequadas criando um clima de impunidade (OLIVEIRA; DANI, 2011).

Urgentemente há a necessidade do poder legislativo brasileiro em tipificar cada vez mais essas novas condutas, especificando cada uma delas de modo singular para que criminosos não saiam impunes pela prática desse tipo de crime. Isto torna-se fundamental e imprescindível para que criminosos não utilizem de lacunas na lei para se beneficiarem e ficarem impunes (OLIVEIRA; DANI, 2011).

A maior carência sobre a legislação brasileira é não possuir itens específicos na lei que determine que os provedores forneçam facilmente à autoridade policial informações, principalmente de *logs*, para o procedimento de investigação nos casos de crimes virtuais. A obrigatoriedade do pedido judicial, conforme determina o Marco Civil da Internet, torna o processo de investigação muito lento (BRASIL, 2016).

A seguir serão destacadas algumas leis brasileiras específicas referente ao crime virtual, ressaltando que muitos dos crimes ocorridos por meio informático são julgados analogamente a outras legislações, em específico o código penal brasileiro.

3.2.1 Lei nº 12.735/2012

Esta lei dispõe sobre mudanças na legislação penal a fim de tipificar algumas condutas praticadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticados contra sistemas informatizados e similares (BRASIL, 2012).

---

[1] "*Modus operandi* é uma expressão em latim que significa 'modo de operação', utilizada para designar uma maneira de agir, operar ou executar uma atividade seguindo sempre os mesmos procedimentos". (INFORMAL, 2010)

Em resumo, esta lei trata da estruturação da polícia judiciária para a construção de equipes especializadas em crimes virtuais, tal como explicita o artigo 4º a seguir:

"Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado" (BRASIL, 2012).

E ainda no seu artigo 5º define que o inciso II do § 3º do artigo 20 da lei nº 7.716/89[2] que trata da prática, indução ou incitamento a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional inclua no tocante a cessação da prática delituosa nos meios de comunicação, sob pena de desobediência, também as formas eletrônicas ou de publicação por qualquer meio (BRASIL, 2012).

3.2.2 Lei nº 12.737/2012

Mais conhecida como Lei Carolina Dieckmann, entrou em vigor em abril de 2013. A referência à atriz se justifica pelo episódio em que fotos íntimas foram roubadas de seu computador e logo em seguida publicadas na *internet* (SERAFIM; LISBOA, 2014).

Segundo Kleina (2012) "A nova lei caracteriza alguns crimes virtuais e penaliza práticas como invadir eletrônicos em geral [...]". A lei 12.737/2012 fez com que algumas alterações fossem realizadas na lei 2.848 de 07 de Dezembro de 1940 (Código Penal Brasileiro).

A lei em questão divide a invasão de dispositivo informático em dois artigos: 154A e 154B, onde:

> Art.154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (BRASIL, 2012a)

[2] Lei que trata dos crimes resultantes do preconceito de raça ou de cor.

Esta lei aplica-se não somente para quem pratica o ato, mas também para quem produz qualquer dispositivo ou programa de computador que tenha como objetivo ou permita a invasão de dispositivo informático (BRASIL, 2012a).

O artigo 154-B traz ainda a complementação sobre o ato da representação:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 2012a)

3.2.3 Lei 9609/1998

"Dispõe sobre a proteção da propriedade intelectual de programa de computador [...]" (BRASIL, 1998).

De acordo com a lei:

> Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. (BRASIL, 1998)

No **capítulo V**, artigo 12 desta lei, encontra-se a descrição e as penalidades a pessoa que violar os direitos de autor de programa de computador estabelecendo pena de seis meses a dois anos ou multa. Infere ainda, àquele que além de violar ainda reproduza, no todo ou em parte, programa de computador para fins de comércio sem autorização, pena de reclusão de um a quatro anos e multa (BRASIL, 1998).

Nesta mesma pena também incorre quem "[...] vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral" (BRASIL, 1998).

3.2.4 Lei nº 11.829/2008

Segundo Brasil (2008) a criação desta lei servirá para “Aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição de tal material [...]”. Devido às deficiências da lei do estatuto da criança e do adolescente, foi sancionada a lei nº 11.829/2008 em complemento a esse estatuto. Foram adicionados alguns artigos que reprimem os casos de pornografia infantil ocorridos por sistemas informáticos ou telemáticos (BRASIL, 2008).

Em resumo esta lei estabelece o seguinte:

- **Crime de produção de pornografia infantil:** estabelecido no artigo 240 refere-se à produção de qualquer material pornográfico envolvendo criança ou adolescente. Incorre neste crime também quem agencia e/ou participa de cenas de pornografia infantil. A pena para este crime é aumentada em casos onde o criminoso exerce função pública, ou se aproveita de relações domésticas, ou se aproveita de relações com a vítima, ou se aproveita de relações com quem tenha autoridade sobre a vítima, ou se pratica o crime com o consentimento de quem tenha autoridade sobre a vítima (FORTES, [2008]).
- **Crime de venda de pornografia infantil:** enquadrado no artigo 241 desta lei, define como crime o ato de vender ou expor à venda foto ou vídeo de pornografia ou sexo explícito envolvendo crianças e adolescentes por qualquer meio incluindo a *internet* (FORTES, [2008]).
- **Crime de divulgação de pornografia infantil:** tipificado no artigo 241-A este crime compreende a publicação, troca ou divulgação por qualquer meio, incluindo também a *internet,* de foto ou vídeo pornográfico com crianças ou adolescentes. A lei agrega a este crime quem assegura o armazenamento das fotos e vídeos de pornografia infantil, sendo responsabilizadas as empresas de *internet* que guardam tais materiais para pessoa que queira divulgar, ou que asseguram o acesso à *internet* da pessoa que praticar esse crime. Contudo, os responsáveis pelo acesso à *internet* somente serão culpados se não cortarem o material pornográfico mediante uma denúncia e uma notificação oficial (FORTES, [2008]).
- **Crime de posse de pornografia infantil:** o artigo 241-B refere-se a “Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” (BRASIL, 2008).
- **Crime de produção de pornografia infantil simulada** (artigo 241-C) é o ato de “Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por

meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual" (BRASIL, 2008).

- **Crime de aliciamento de criança:** (artigo 241-D):

> [...] é o ato de aliciar, assediar, instigar ou constranger a criança (menor de 12 anos de idade), por qualquer meio de comunicação (pessoalmente ou à distância: pelo telefone, internet, etc.), a praticar atos libidinosos, ou seja, passa a ser crime convidar ou "cantar" uma criança para relação libidinosa (sexo, beijos, carícias, etc.). É muito comum esse tipo de assédio pela internet, através de salas de bate-papo (chats) ou programas de relacionamento [...]. (FORTES [2008])

Também incorre neste crime quem "[...] facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfico com o fim de com ela praticar ato libidinoso" (BRASIL, 2008). E quem induz a "[...] criança a se exibir de forma pornográfica ou sexualmente explícita" (BRASIL, 2008).

E, por fim, esta lei no seu artigo 241-E define:

> [...] a expressão "cena de sexo explícito ou pornográfica" como sendo aquela que registra "qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (BRASIL, 2008)

3.2.5 Lei 12.965/2014

A lei conhecida como Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil determinando diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação aos direitos e deveres de cada um dentro da rede mundial de computadores de forma a garantir a segurança, a privacidade e a neutralidade respeitando os direitos individuais presentes na Constituição Federal de 1988 (BRASIL, 2014).

Esta lei veio a assegurar, entre outras coisas, o princípio da inviolabilidade da vida privada e da intimidade dentro da *internet*. Importante ressaltar que, anteriormente a essa lei, o ordenamento jurídico relativo a esse tema era deficiente para os casos ocorridos dentro da rede (GALO, [2014]). "Além disso, o Marco Civil garante o sigilo de informações, comunicações, dados e registros armazenados, exceto quando o usuário expressar e informar o consentimento

da utilização de seus dados, ou por determinação judicial, ou hipóteses previstas em lei" (GALO, [2014]). Todas esses garantias e direitos do usuário estão expressos no art. 7º dessa lei que reforça o direito à privacidade e à liberdade de expressão, tornando nula qualquer cláusula contratual que se oponha a esses direitos concorrendo com o art. 10 que atribui às empresas que fornecem o acesso à *internet* a responsabilidade pela proteção, sempre preservando a honra, a vida privada e a imagem dos usuários, de quaisquer dados e registros pessoais, armazenamento dos registros de conexão e acessos às aplicações, somando-se ainda, a responsabilidade por danos que resultarem de conteúdo gerado por terceiros (BRASIL, 2014).

Vale ressaltar que o art. 11 estabelece que, em quaisquer condições ditas anteriormente referente a coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de *internet*, desde que ao menos um desses atos seja realizado no Brasil estará em vigor a legislação brasileira e as empresas deverão, quando solicitadas, fornecer as informações requeridas pela justiça (BRASIL, 2014).

Portanto, sem prejuízo das demais sanções cíveis, administrativas ou criminais, o art. 12 designa sanções àqueles que infringirem os artigos 10 e 11 dessa lei:

> [...]
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País. (BRASIL, 2014)

Os artigos que seguem na lei ainda determinam o tempo guardar dados, informações e registros de conexões dos usuários pelo prazo de um ano em ambiente controlado e seguro não podendo transferir a responsabilidade para terceiro, conforme art. 13. E tratando-se de

acesso às aplicações, o respectivo registro deverá ser guardado pelo prazo de 6 meses sob sigilo e em local seguro pelo provedor de aplicações de *internet*, art. 15 (BRASIL, 2014).

3.3 INVESTIGAÇÃO PREVENTIVA E REPRESSIVA

Os métodos descritos nesse capítulo foram baseados exclusivamente nos modelos de investigação reproduzido no curso **Crimes Cibernéticos: procedimentos básicos** formulados pela Secretaria Nacional de Segurança Pública – Brasil.

Sempre da ocorrência de um crime virtual torna-se necessária uma investigação a fim de, prover a um futuro processo fundamentos precisos sobre o apontamento de supostos criminosos. Os membros de uma equipe de investigação podem utilizar diversos recursos no processo de investigação, no entanto, em muitos casos, os criminosos se mostram publicamente na *internet*. E diante dessa vantagem é possível realizar a identificação do criminoso, a sua localização bem como a identificação dos crimes cometidos (BRASIL, 2016).

Um processo muito importante realizado por equipes de investigação é o que é chamado de **"busca sistemática"**. Esse modelo de investigação de crime na *internet* é uma forma de investigação preventiva, dependendo apenas da iniciativa da autoridade policial, onde são identificados responsáveis por diversos tipos de crimes. Observa-se que, a falsa sensação de anonimato provocada pela *internet*, facilita esse tipo de investigação. Contudo, a equipe de investigação tem que definir parâmetros e impor limites a este tipo de investigação, já que o grande volume de informação pode gerar lentidão ao processo e tomar muito tempo (BRASIL, 2016).

Para esse tipo de investigação é indispensável que o investigador crie contas e perfis falsos de vários serviços na *internet* para serem usados no momento da investigação tais como *e-mail*, *chats*, redes sociais, entre outros. Essas contas devem possuir fotografias e dados que passem impressão de ser realmente verdadeiro. E um dos fatores mais importantes é possuir uma Estória Cobertura (EC)[3]. A partir desse ponto, pode-se conseguir realizar a infiltração

[3] Termo utilizado em Inteligência Policial para expressar uma estória falsa, criada por um agente investigador infiltrado no ambiente criminoso com intuito de obter informações sobre o crime e o criminoso, que cubra todas as possibilidades de questionamento de um investigado com o qual manterá contato na Internet, mas que, ao mesmo tempo, não exponham pessoas inocentes (BRASIL, 2016).

virtual em gangues, torcidas organizadas, quadrilhas ou mesmo identificar pedófilos, obtendo, assim, informações altamente relevantes para a prevenção e repressão ao crime (BRASIL, 2016).

Outro modo de investigação é a utilização de **fontes abertas** na identificação de alvos em crimes virtuais. Esse método consiste em obter informações sobre determinadas atividades, produto ou indivíduo procurando em fontes de informações que sejam livres e gratuitas na *internet* (BRASIL, 2016).

> As fontes abertas podem ser utilizadas em várias situações em uma investigação criminal. A identificação de membros de organizações criminosas é uma das mais importantes e que trazem melhores resultados ao trabalho policial, tendo em vista que há comunidades virtuais onde os criminosos se apresentam, expõem seu pseudônimo e o nome da organização criminosa a que pertencem. (BRASIL, 2016, p. 5)

As fontes abertas formais que detêm informações altamente confiáveis como jornais, revistas, diários oficiais, sites governamentais e/ou corporativos, ou informais onde as informações podem ser inseridas por qualquer pessoa como o *Facebook*, *blogs*, fóruns de discussão e redes sociais, conseguem identificar exatamente, juntamente com o apoio de outros sistemas de informação e identificação civil, muitos criminosos na *internet* (BRASIL, 2016).

No entanto, quando se fala de *malwares* – *softwares* maliciosos – para a prática de crimes, o tratamento dado pelas autoridades consiste em tentar rastear a origem do crime fazendo uma análise do *malware* passo-a-passo. Esta análise é realizada em um ambiente virtual isolado e exclusivo para essa prática e sendo feito apenas por pessoas capacitadas, tais como peritos criminais da área da informática ou especialistas na área que possuam uma infraestrutura adequada (BRASIL, 2016).

As ferramentas mais úteis para a investigação nesse tipo de caso são *softwares* que analisam quais arquivos e registros do sistema são acessados pelo *malware*. A ferramenta mais capacitada são os ***sniffers*** que conseguem capturar, registrar e analisar os dados que trafegam pelo sistema de comunicação à procura de tráfego suspeito (BRASIL, 2016).

> Essas ferramentas vão ajudar a autoridade a identificar qual o ponto de comunicação do *malware* com o mundo exterior, ou seja, para onde ele envia as informações que

> colhe. Pode ser uma conta de e-mail, um servidor de arquivos, um banco de dados clandestino, um site na Internet ou qualquer aparato que possa guardar as informações furtadas de forma segura para que sejam acessadas posteriormente pelo criminoso. Esse trabalho é denominado "análise comportamental do *malware*". Além disso, também pode ser efetuada, com ferramentas específicas, a chamada "engenharia reversa", que é a análise do código do software para entender seu funcionamento. (BRASIL, 2016, p. 7)

O capítulo 4 tratará mais especificamente algumas ferramentas eficazes para o direcionamento da investigação no caso de crime virtual ocorrido na rede de computadores. A seguir, será tratado da forense computacional que é o método específico contribuinte para a investigação e fornecedor de maior credibilidade às informações extraídas para o apontamento de crimes.

3.4 PERÍCIA FORENSE COMPUTACIONAL

Com o decorrer dos anos, grandes modificações nos aspectos políticos, sociais, econômicos e culturais tiveram origem principalmente pelo avanço da informática que trouxe uma grande mudança na forma como os seres humanos se relacionam. Cada vez mais a sociedade moderna torna-se dependente da internet como forma de difusão da informação, pois a facilidade e a velocidade em que a informação circula ocasionaram muitas vantagens e oportunidades às pessoas (SÔNEGO, 2012).

A facilidade de interação nos meios de comunicação oportunizando realizações de transações bancárias, consultas de qualquer tipo de informação e troca de mensagens com o mundo todo, atraiu a ação de criminosos que viram na internet possibilidades infinitas de fraudar e roubar informações utilizando de muitos meios fraudulentos para a prática de crimes dentro do mundo virtual (SÔNEGO, 2012).

A tecnologia dos computadores está diretamente envolvida com o aumento de atividades ilícitas, pois, além de serem utilizados como mecanismos de práticas de crimes relacionados diretamente ao computador, ainda podem conter evidências com qualquer outro tipo de atividade ilícita, incluindo homicídio e estupro. Esse aumento exponencial dos crimes relacionados com os computadores requer uma análise diferenciada de como se obter e utilizar as evidências digitais do crime armazenadas nos computadores. Tal procedimento é necessário para o esclarecimento do crime e apenas pode ser realizado através de metodologias da forense computacional (REIS; GEUS, [2002?]).

Freitas (2003, p. 7) afirma que a perícia forense computacional compreende “[...] o processo de coleta, recuperação, análise e correlacionamento de dados que visa, dentro do possível, reconstruir o curso das ações e recriar cenários completos fidedignos”.

Discursando sobre o tema, Eleutério e Machado (2011, p. 31 apud GONÇALVES et al, 2012, p. 2, 3) afirmam que, “a computação forense é a ciência que, através de técnicas e habilidades especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio de praticá-lo”. Os autores mencionam inclusive que, esta modalidade de perícia envolve a polícia dentro de um trabalho investigativo e pericial na resolução de crimes cometidos através do uso do computador. Sendo que, a perícia computacional pode ser usada tanto para fins legais como exemplo investigar espionagem industrial, como também utilizada para ações disciplinares internas, tendo como exemplo, o uso indevido de recursos de uma empresa (ELEUTÉRIO; MACHADO, 2011 apud GONÇALVES et al, 2012).

3.4.1 Evidência digital

Evidentemente, após se ter o conhecimento sobre o crime, torna-se necessária a busca por evidências que possam direcionar a investigação como forma de provar a autoria do crime. Em qualquer procedimento de busca e apreensão no ambiente de crime, os agentes da lei têm a obrigação de realizar a busca incessante por provas. E quando o crime envolve recursos digitais pode-se, então, falar em evidência digital (BRASIL, 2016).

Evidência digital caracteriza-se como “qualquer informação de valor probatório, que é armazenado ou transmitido de forma digital” (BRASIL, 2016). Essa informação é capaz de determinar se um sistema computacional sofreu uma violação, ou pelo menos, que provê uma ligação com a vítima ou com o autor do crime (CANDIDO JUNIOR; SAÚDE, 2005). Como exemplo podem ser citados “[...] arquivos, fotos, vídeos, históricos armazenados em um disco rígido de um computador, vídeo digital, áudio digital, pacotes transmitidos pela rede de comunicação, entre outros” (BRASIL, 2016).

É importante ressaltar que, devido à grande volatilidade das evidências digitais, é imprescindível, segundo Rosa (2011), que as informações devam ser preferencialmente coletadas obedecendo sua ordem de volatilidade no sistema. A autora enfatiza que alguns

dados têm chance maior de se perderem por estar armazenados em dispositivos voláteis, à medida que, são mais sensíveis à corrupção durante o processo de coleta, devendo sempre, ao se realizar tal processo, considerar o ciclo de vida esperado dos dados (ROSA, 2011). A seguir, Oliveira (2007, p. 28) elenca as principais fontes de dados em um sistema computacional em ordem descendente de volatilidade:

- Dispositivos de armazenagem da CPU (registradores e caches);
- Memória de periféricos (memória de video, por exemplo);
- Memória principal do sistema;
- Tráfego de rede (pacotes em trânsito na rede);
- Estado do sistema operacional (como, por exemplo, estado das conexões de rede e dos processos em execução, usuários logados e configurações do sistema);
- Módulos de *kernel;*
- Dispositivos de armazenagem secundária;
- Sistema de arquivos;
- Arquivos de *log*.

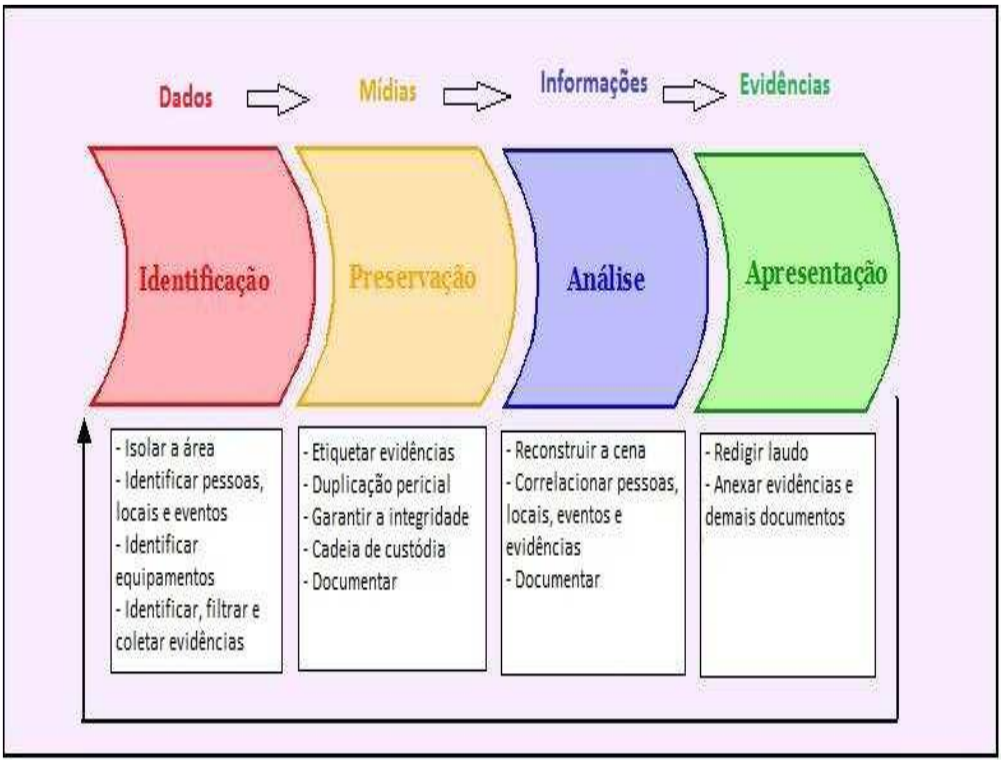
3.4.2 Procedimentos da forense computacional

Rosa (2011) destaca que dados obtidos com a busca de evidências devem ser autênticos e íntegros, e para assegurar a veracidade das informações encontradas faz-se necessária a elaboração de métodos e procedimentos adequados e bem definidos. A autora salienta também a importância de documentar precisamente e rigidamente todo o processo forense, de modo a manter os caminhos seguidos e registrar todos os indivíduos envolvidos no processo de investigação.

O processo de investigação forense assegura também que as evidências analisadas não foram alteradas ou contaminadas no decorrer de todo o procedimento já realizado (CASSEY, 2000 apud OLIVEIRA, 2007). “[...] É importante que a investigação seja conduzida de maneira metódica, bem organizada e em sintonia com a tecnologia envolvida” (CASSEY, 2000 apud OLIVEIRA, 2007, p.33, 34).

Segundo Freitas (2006, p. 2) “A perícia forense computacional possui quatro procedimentos básicos: todas as evidências devem ser identificadas, preservadas, analisadas e apresentadas”. A Figura 2 evidencia os quatro procedimentos básicos para a realização da perícia forense computacional.

Figura 2: procedimentos da forense computacional



Fonte: Rosa (2011, p. 40).

3.4.2.1 Identificando as evidências

Nesta fase, cabe ao perito buscar e relacionar todas as evidências possíveis, levando em consideração o tipo do crime ocorrido, pois cada tipo de crime apresenta evidências particulares (ROSA, 2011). Freitas (2006) reforça que em cada tipo de crime investigado as evidências podem variar, o autor cita como exemplo casos de crimes de pedofilia ou pornografia, onde certamente o perito buscará por vestígios do tipo imagem ou vídeo prioritariamente.

Rosa (2011) salienta que o perito no processo de identificação das evidências deve procurar basicamente por informações próximas ao acontecimento, ligar nomes a pessoas, datas e, claro, obter informações sobre o sistema que fora afetado. Ao referir-se a esse assunto, Cagnani e Santos ([2007?]) complementam que o perito deve visualizar como iniciará os seus trabalhos, qual é o tipo de dado a ser buscado e coletado e reavaliar com a equipe se os dados capturados na investigação são importantes para acusações ou defesas de suspeitos e vítimas.

A coleta de dados é realizada logo após o processo de identificação das fontes de evidências, para tal, deve-se seguir uma ordem de acordo com a volatilidade das informações capturadas (ROSA, 2011).

Freitas (2006, p. 2) determina como encontrar possíveis evidências da seguinte maneira:

> - Procurar por dispositivos de armazenamentos (*hardwares*): *laptops*, Hds[4], disquetes, CDs[5], DVD[6]s, *drivers* Zip/Jaz, *memory Keys*, *pendrives*, câmeras digitais, MP3 *player*, fitas DAT[7], *Pocket* PC[8], celulares, dispositivos de backup ou qualquer equipamento que possa armazenar evidências;
> - Procurar por informações relacionadas ao caso: anotações, nomes de pessoas, datas, nomes de empresas e instituições, números de telefones, documentos impressos etc.;
> - Distinguir entre evidências relevantes e irrelevantes em uma análise ao vivo.

3.4.2.2 Preservando as evidências

"As evidências devem ser preservadas de modo que não haja dúvidas sobre sua veracidade" (ROSA, 2011, p. 17).

De acordo com Cagnani e Santos ([2007?]) a perícia não deve ser realizada nos dados originais apreendidos, ou seja, o primeiro passo a ser seguido na realização de uma perícia computacional é o de gerar uma imagem exata da mídia original e fundamentar todos os trabalhos sobre esta imagem, os dados originais devem ser preservados até o dia do julgamento do processo a que estão vinculados. Os autores enfatizam sobre a obrigatoriedade e responsabilidade do perito em registrar os materiais recebidos, os acessos a estes materiais, as pessoas que tiveram contato com as evidências devendo sintetizar qual o motivo para realização deste contato.

Alguns cuidados devem ser tomados para evitar o comprometimento, substituição ou perda das evidências, de acordo com Freitas (2006) e Rosa (2011):

---

[4] *Hard Disk*

[5] *Compact Disc*

[6] *Digital Versatile Disc*

[7] *Digital Audio Tape*

[8] *Personal Computer*

- A criação de imagens para investigação;
- A importância de salvar os dados em mídias não regraváveis;
- Lacrar sacos e etiquetá-los;
- As evidências coletadas deverão ser armazenadas em local seguro;
- Documentar toda e qualquer mudança da evidência (Cadeia de custódia).

Uma técnica bastante relevante para preservar e certificar-se de que a informação não será alterada após a coleta é a utilização de uma assinatura digital. A assinatura digital pode ser gerada por uma "função *hash*", que cria um código único gerado para cada conteúdo sobre o qual é aplicado. Desta forma, sempre que for aplicada a função *hash* sobre o mesmo conteúdo o código será igual identificando-o unicamente. Caso a informação for alterada o código mudará e a evidência poderá ser questionada no processo judicial. (BRASIL, 2016)[9].

3.4.2.3 Analisando as evidências

De acordo com Rosa (2011) esta é a fase de maior demora no processo geral da perícia forense computacional, o perito é a peça chave desta fase, cabem a ele as tarefas de reconstrução do cenário do crime, caso seja possível, elaboração de relações entre as evidências e eventos coletados no decorrer da investigação e responder questões que estão diretamente relacionadas à perícia forense. A autora determina também a importância de manter documentadas todas as atividades que foram realizadas nesta fase.

Oliveira (2007) salienta que a fase de análise das evidências é à hora de examinar todo o material coletado, permitindo assim, a elaboração de conclusões do crime originário de toda a investigação.

Esta fase é descrita por Cagnani e Santos ([2007?]) como, talvez, a mais dificultosa, pois existem inúmeros tipos de arquivos a serem analisados, dentre eles são citados os arquivos com extensão JPG[10], AVI[11] e doc[12], estes documentos são representações de

[9] Um aplicativo gratuito capaz de realizar a função *hash* e validação das evidências é o WinMD5Free (BRASIL, 2016).

[10] *Joint Photographic Experts Group*

[11] *Audio Video Interleave*

[12] *Document*

imagens, vídeos e documentos de texto, respectivamente. Os autores também apontam a esteganografia como sendo uma das técnicas mais utilizadas para esconder dados.

Freitas (2006, p. 4) acredita que a principal característica e objetivo da análise das evidências é "tentar identificar quem fez, quando fez, que dano causou e como foi realizado o crime". O autor segue discursando que após o término das análises é possível que se tenha respostas para as seguintes questões:

- Qual a versão do Sistema Operacional que estava sendo investigado?
- Quem estava conectado ao sistema no momento do crime?
- Quais arquivos foram usados pelo suspeito?
- Quais portas estavam abertas no Sistema Operacional?
- Quem *logou* ou tentou *logar* no computador recentemente?
- Quem eram os usuários e a quais grupos pertenciam?
- Quais os arquivos foram excluídos?

3.4.2.4 Apresentando a análise

Para que sejam apresentados os resultados obtidos na investigação faz-se necessária a criação do laudo pericial, que basicamente é a descrição que o perito realiza após ter as correlações das evidências e análises. Este laudo tem a obrigatoriedade de ser redigido de forma clara, organizada, concisa, imparcial e conclusiva (ROSA, 2011).

Freitas (2006, p. 5) descreve o laudo pericial como sendo "[...] um relatório técnico sobre a investigação, onde são apontados os fatos, procedimentos, análises e resultado". O autor ainda estabelece algumas características desta fase:

> - O laudo deve ser claro, conciso, estruturado e sem ambiguidade, de tal forma que não deixe dúvida alguma de sua veracidade;
> - Deverão ser informados os métodos empregados na perícia, incluindo os procedimentos de identificação, preservação e análise, e os softwares e hardwares utilizados;
> - O laudo pericial deve conter apenas afirmações e conclusões que possam ser provadas e demonstradas técnica e cientificamente. (FREITAS, 2006, p. 5)

Cagnani e Santos ([2007?]) reforçam que esta última etapa, em que as evidências coletadas e já analisadas são entregues e apresentadas às autoridades pertinentes, necessita de alguns requisitos fundamentais para a imparcialidade do laudo pericial, resumindo-se em confiabilidade, habilidade e isenção do perito.

Por fim, Rosa (2011) argumenta que o laudo deve ser elaborado com um linguajar a quem se destina, não deixando de utilizar também linguagens gráficas e visuais, pois estas facilitarão para uma melhor compreensão de todos. A autora lembra também que todas as argumentações contidas no laudo devem possuir embasamento, pois o laudo pericial pode ser questionado e contestado.

4. SOFTWARES FORENSES EM REDES DE COMPUTADORES

Este capítulo tem por objetivo demonstrar o funcionamento de alguns softwares que podem ser utilizados para investigações nos casos de crime virtual contribuindo, desta forma, para a forense computacional. As ferramentas utilizadas são destinadas a captura de dados na rede de computadores a fim de, direcionar a investigação. Estas ferramentas por si só, obviamente, não são conclusivas para o apontamento real do infrator de determinadas infrações ou crimes, necessitando de interpretação do perito criminal, investigador ou pessoa constituída para isso, confeccionando assim, o laudo pericial como peça probatória.

As ferramentas estudadas nesse capítulo foram escolhidas devido à presença em várias referências pesquisadas durante a elaboração do trabalho incluindo fontes ligadas a segurança em redes de computadores e forense computacional, entre elas podem-se citar VARGAS (2007), (2011); SILVA (2013); LYON (2008); VIEIRA (2011); cabendo ressaltar, como fator muito importante, que algumas das ferramentas a serem evidenciadas a seguir foram mencionadas no curso Crimes “Cibernéticos: procedimentos básicos” realizado pela SENASP, subsidiária desse curso, entre outras fontes.

É importante destacar que o propósito desse capítulo não é realizar uma análise pormenorizada das ferramentas aludidas posteriormente, mas sim trazer ao conhecimento geral como forma a apresentar detalhes importantes do modo de funcionamento de tais ferramentas. Obviamente, existem muitas mais ferramentas que podem ser utilizadas para a realização da investigação ou da perícia forense computacional que não estão arroladas nesse trabalho, no entanto as ferramentas aqui reportadas estão ligadas diretamente com o tema proposto condizente à procura de dados relevantes para a investigação dentro das redes de computadores.

4.1 CALLERIP

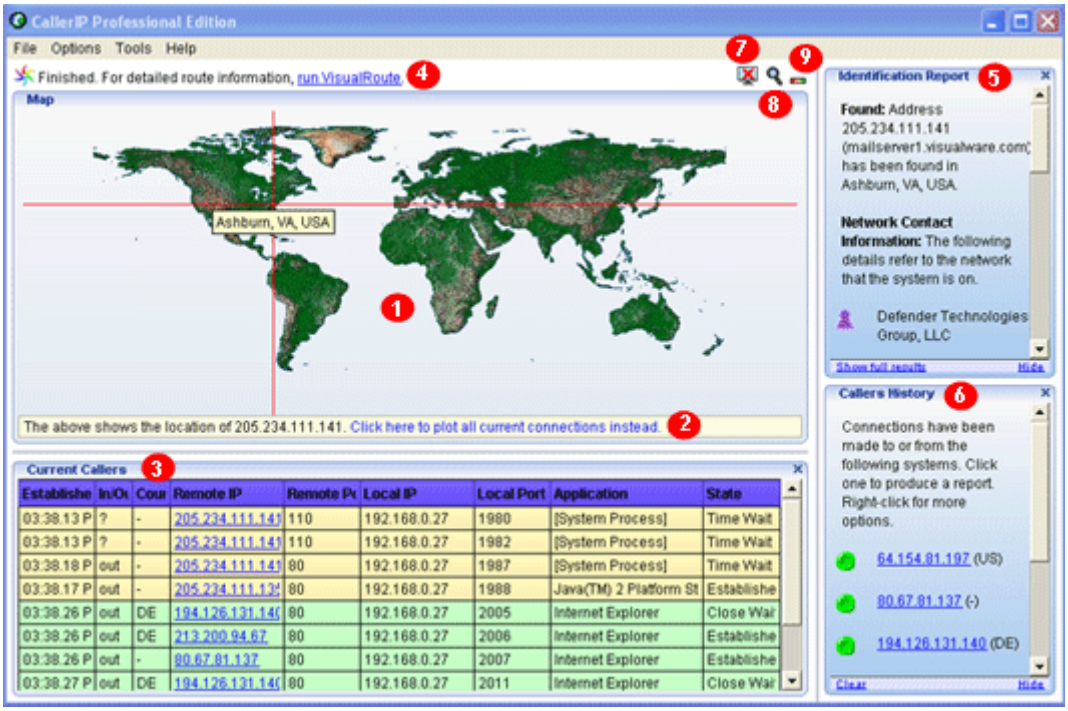
A ferramenta *CallerIP* tem a função de auxiliar na indicação de entradas, saídas e invasões de IP na máquina em que estiver instalado. Este programa tem a finalidade de informar qual o IP que está conectado ou tentando se conectar, mostrando em um mapa mundi qual a sua localização juntamente com endereço, telefone e o responsável por aquele IP (VARGAS, 2007).

Este *software* pode ser utilizado também para a investigação de funcionários que estão utilizando de aplicações que facilitam o acesso à rede interna de computadores, tornando-a vulnerável. Desta forma, essa ferramenta é utilizada para monitorar as entradas e saídas dos IPs do sistema operacional, de forma a identificar qual a aplicação está sendo utilizada para esse tipo de prática (VARGAS, 2007).

Com o *CallerIP* também há a possibilidade de monitoramento de atividades das portas que estão abertas no sistema que geralmente não estão protegidas por *firewalls*. Desta forma, essa ferramenta pode identificar a invasão antes que o sistema ou as informações sejam prejudicados. Informações do tipo porta remota, IP remoto e identificação do processo estão presentes nessa ferramenta e facilitam a identificação de intrusos e quais portas devem ser fechadas para acabar com as tentativas de intrusão (VISUALWARE, 2014a).

A Figura 3 mostra a tela principal do *CallerIP* evidenciando detalhes importantes da ferramenta.

Figura 3: Tela principal do *CallerIP*



Fonte: VISUALWARE (2014b).

A numeração na Figura 3 indica várias características da tela principal do *CallerIP*. Seguem os detalhes da ferramenta conforme o fabricante *Visualware*:

1. **Mapa mundi.** Nesse quadro, representado pelo mapa mundi, quando uma conexão for estabelecida é mostrado o local exato de onde a ligação foi originada. De modo a facilitar a identificação das tentativas de invasão, todos os locais de conexão IP são mostrados no mapa, onde cada endereço de conexão apontado no mapa mostrará no seu local de origem todos os endereços IPs encontrados (VISUALWARE, 2014c).

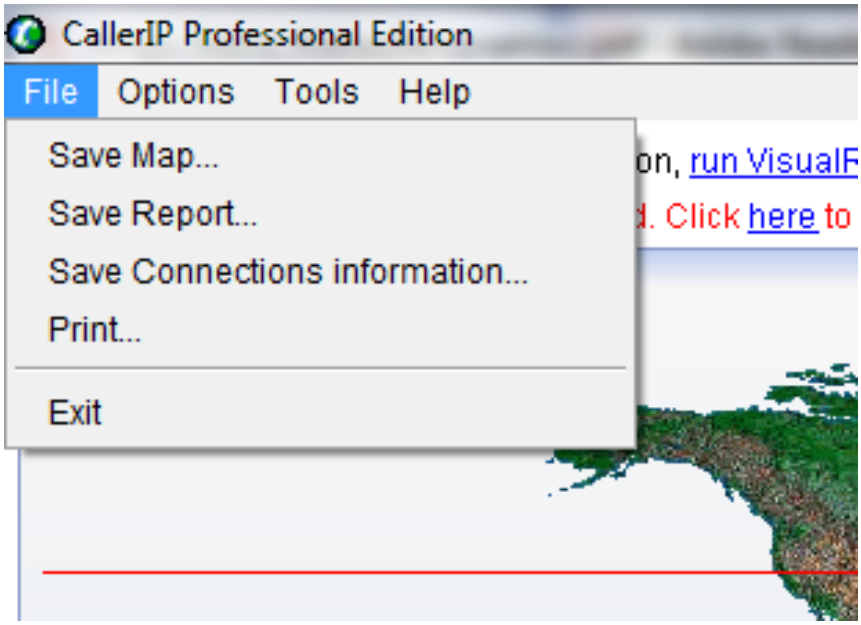
2. **Traçar todas as conexões.** Quando esse botão é clicado, aparecerão no mapa em forma de mira, todas as conexões atualmente realizadas. Cada mira representa um país de origem da conexão e ao posicionar o *mouse* nessa mira são apresentadas todas as conexões IP do país em questão (VISUALWARE, 2014b).

3. **Tabela de conexões.** Nessa tabela são encontrados dados importantes das conexões que estão em evidência atualmente na máquina onde o *CallerIP* está sendo executado. Incluem-se nessa tabela informações do tipo: país de origem da conexão, se a ligação é de entrada ou saída, endereço IP remoto, endereço IP local, número da porta, a aplicação que está se comunicando e o estado da conexão (VISUALWARE, 2014b).

4. **Aplicar *VisualRoute*.** Se o usuário possuir a ferramenta *VisualRoute* instalada em complemento com o CallerIP, poderá refinar ainda mais o rastreamento das conexões. O *VisualRoute* também é de fabricação da *Visualware* (VISUALWARE, 2014b).
5. **Relatório de Identificação.** Após escolher um IP na tabela de conexões (item 3 da Figura 3), é possível analisá-lo obtendo um relatório com as informações referentes ao IP selecionado (VISUALWARE, 2014b). Este relatório fornece o endereço IP registrado ao domínio analisado juntamente com os endereços de *e-mails* e números de telefone. Desta forma, é possível às autoridades rastrearem o criminoso mais facilmente (VISUALWARE, 2014d).
6. **Histórico de Conexões.** Nessa janela é mostrado o histórico de chamadas com o endereço IP buscado que geraram os relatórios de identificação, e se clicados, novamente geram um novo relatório. Ao lado esquerdo do endereço IP há um sinalizador que identifica a periculosidade da ameaça, sendo a cor verde utilizada para identificar que a conexão realizada não representa perigo de *hacker*; a cor âmbar representa que há algum risco que seja um *hacker*; e a cor vermelha representa que aquela conexão tem muita probabilidade de ser um *hacker*. Os endereços de IP dessa janela ainda permitem o clique com o botão direito do *mouse* mostrando três opções: a primeira "*Look up*" permite traçar a localização do IP no mapa e criar um novo relatório de identificação; a segunda "*Search log for*" permite uma busca pelos registros da ferramenta à procura daquele endereço IP; e a terceira "*Add alarm*" permite ao usuário definir um alarme para quando o endereço IP clicado se conectar à máquina novamente (VISUALWARE, 2014e).
7. **Ícone do servidor *CallerIP*.** Este ícone direciona para a configuração das preferências do servidor de *CallerIP*, permitindo, após a configuração, o monitoramento remoto através do navegador (VISUALWARE, 2014b).
8. **Ícone de pesquisa de registro.** Este ícone direciona para uma caixa de diálogo que permite a pesquisa de registros de conexões informando os parâmetros manualmente (VISUALWARE, 2014f).
9. **Minimizar a tela.** Este botão minimiza a tela tornando-a condensada mostrando pelas cores identificadoras das ameaças as conexões evidentes (VISUALWARE, 2014b).

Para manter os registros e salvar as informações analisadas existem três opções de salvamento e ainda, uma opção de imprimir a tela, conforme a Figura 4:

Figura 4: Opções do CallerIP



Fonte: VISUALWARE (2014h).

A opção ***"Save Map"*** permite ao usuário salvar o mapa atual visualizado. A opção ***"Save Report"*** dá ao usuário a oportunidade de salvar a exibição do relatório atual. E a opção ***"Save Connections information"*** permite ao usuário salvar as conexões atuais. Por fim, a opção ***"Print"*** permite ao usuário imprimir a tela do *CallerIP* (VISUALWARE, 2014g). É importante mencionar que o *CallerIp* não possui código-fonte aberto e não sendo livre é necessário a compra de uma licença para a sua utilização.

4.2 EMAILTRACKERPRO

Grande parte dos *e-mails* recebidos é *spam*. Podendo ser inofensivo de forma a irritar o usuário ou malicioso de modo a conter vírus e tentativas enganosas de obtenção de dados pessoais levando a fraudes de identidade, o *spam* está muito difundido pela *internet*. Deste modo, a ferramenta *eMailTrackerPro,* tem a capacidade de rastrear estes *e-mails* maliciosos utilizando-se do cabeçalho do *e-mail* para a pesquisa obtendo informações importantes para a investigação. O *eMailTrackerPro* também possui a funcionalidade de filtrar *spam* analisando

os *e-mails* que chegam avisando o usuário se o *e-mail* é suspeito ou não de *spam* (VISUALWARE, 2014i).

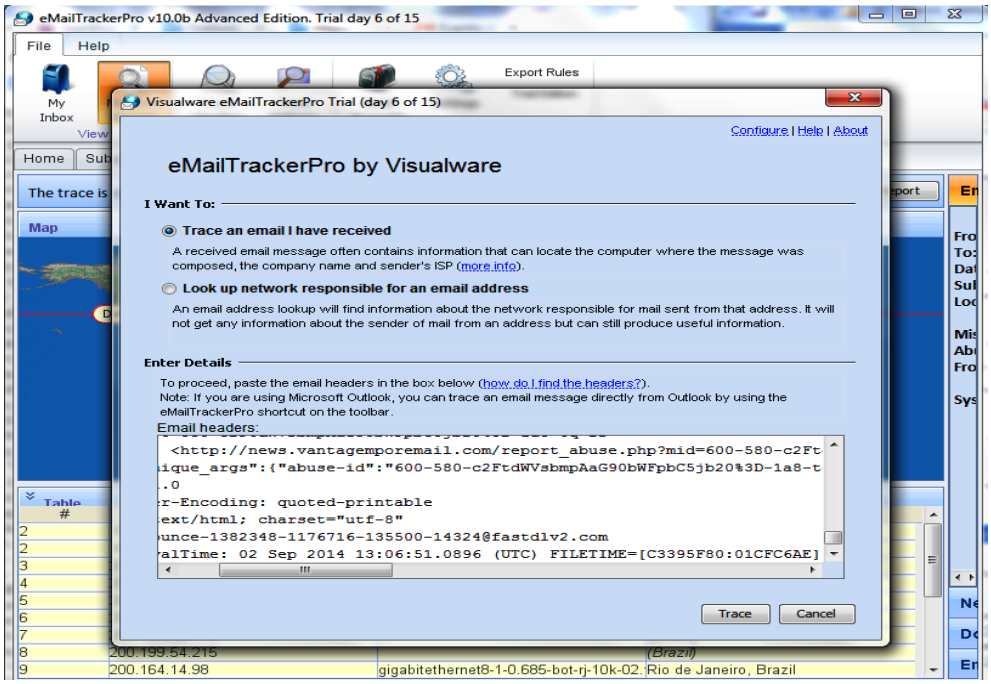
Criada e distribuída pela empresa Visualware, a ferramenta viabiliza informações do local de origem do *e-mail*, onde foi criado, a rota dos locais por onde passou e o nome da organização responsável identificada com seu endereço, telefone, entre outros dados. Toda essa pesquisa ocorre através de uma entrada de *e-mail* ou uma lista de *e-mails* que o usuário insere (VARGAS, 2011a). Vargas (2011a, p. 26) frisa ainda que esta ferramenta pode ser utilizada "[...] quando se deseja, por exemplo, investigar se as informações confidenciais de uma suposta organização foram vendidas antes mesmo de chegar 'às mãos' da empresa responsável por este serviço". O autor comenta que em casos como este, "[...] faz-se uma busca da rota por onde este e-mail passou, informando quando houve o desvio da informação confidencial" (VARGAS, 2011a, p. 26).

A fabricante Visualware (2014i) destaca três principais características do *eMailTrackerPro* explicando alguns detalhes:

- **Traçar um *e-mail* usando o cabeçalho de *e-mail*.** Para fazer melhor uso do *eMailTrackerPro* se faz necessário traçar o cabeçalho de *e-mail*, e não o endereço de *e-mail* somente. Essa instrução justifica-se pelo fato do cabeçalho de *e-mail* possuir informações por onde o *e-mail* tem viajado trazendo informações mais precisas do emissor do *e-mail*, enquanto o simples endereço de *e-mail* sempre executará o rastreamento para o servidor do *e-mail*. Como exemplo, a fabricante menciona que, um endereço de *e-mail* como "anyone@hotmail.com" só irá executar o rastreamento em "hotmail.com", contudo o rastreamento a partir do cabeçalho trará informações fiéis sobre o endereço completo.
- **Filtro de spam.** Esta funcionalidade impede que os *e-mails* de *spam* cheguem à caixa de entrada do usuário. Após informar definições ao protocolo de *e-mail* do servidor do usuário ao *eMailTrackerPro* são realizadas técnicas de captura de *spam* que filtram e apagam os *e-mails* antes deles chegarem a caixa de entrada do usuário.
- **Reportar abuso.** Com esta função é possível enviar relatórios de abusos dos *spams* que o usuário recebe. O *eMailTrackerPro* gera um relatório que é possível enviar ao provedor de *e-mail* com a finalidade de fechar aquela conta maliciosa.

A Figura 5 traz a tela principal de rastreamento de *e-mail* do *software eMailTrackerPro*. Para realizar a busca pelo cabeçalho deve-se escolher a opção *"Trace an email I have received"* onde haverá o espaço necessário para escrever todo o cabeçalho do *e-mail.* Nessa opção, o usuário tem um detalhamento mais exato sobre o real remetente do *e-mail*. O usuário ainda tem a opção de realizar a busca pelo responsável sobre um endereço de *e-mail*, a opção para este tipo de busca é *"Look up network responsible for an email address"*. Depois de selecionada essa opção o usuário terá um detalhamento apenas sobre o servidor do endereço pesquisado (VISUALWARE, 2014j) Na Figura 5 foi escolhida a opção de rastreamento pelo cabeçalho, escrito os parâmetros necessários para a pesquisa e clicado no botão "*Trace*".

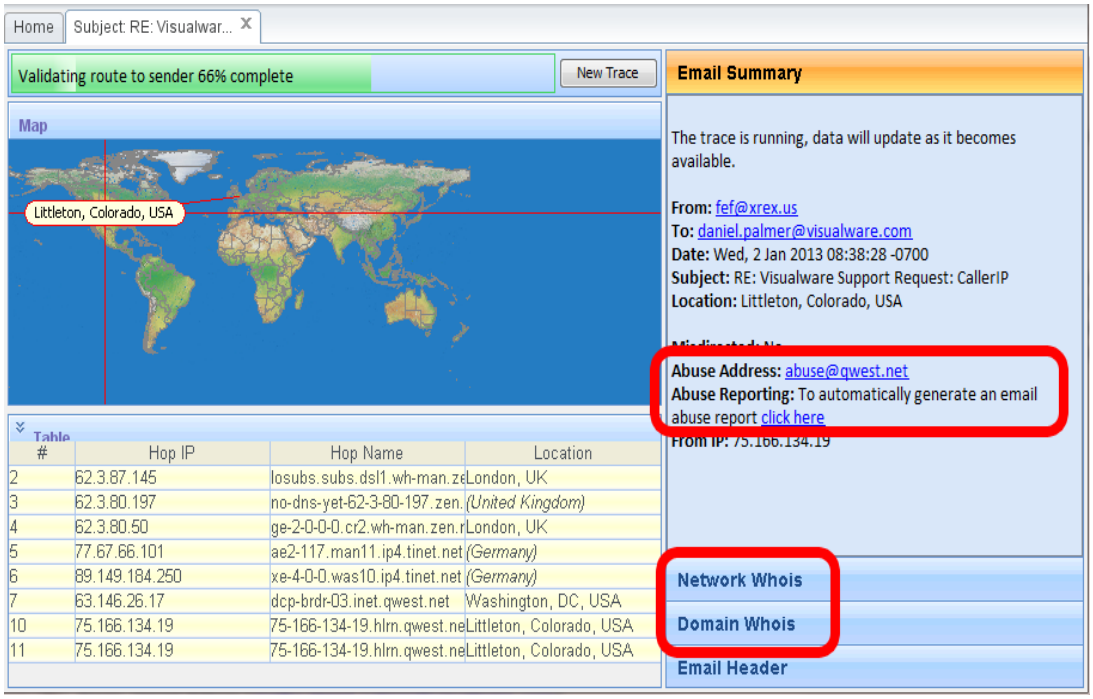
Figura 5: Busca pelo cabeçalho



Fonte: VISUALWARE (2014l).

Após iniciado o rastreamento uma nova aba é aberta para relacionar os dados obtidos com a busca atual. A provável localização da origem do *e-mail* aparecerá no mapa mundi e a tabela de rotas começará a ser preenchida com os endereços de IP por onde a mensagem passou. Sendo que o primeiro registro de IP é do computador onde se está realizando a busca e o último registro IP será a origem mais provável do remetente do *e-mail* (VISUALWARE, 2014). A situação indicada é observada na Figura 6:

Figura 6: Busca em andamento



Fonte: VISUALWARE (2014k).

Uma observação importante mencionada pela fabricante é a impossibilidade de encontrar o nome, número do endereço, telefone exato da casa ou sala de onde foi enviado o *e-mail* devido esses dados somente serem obtidos com ordem judicial, uma vez que viola a lei de proteção de dados e só pode ser obtido pelo provedor de serviços de internet responsável pelo *e-mail* em questão. No entanto, se o usuário quiser agir contra um *e-mail spam* a ferramenta disponibiliza a informação necessária para fazê-lo. As duas áreas marcadas acima mostram o endereço disponibilizado para relatar abusos e duas seções sobre informações *Whois* (VISUALWARE, 2014k). Salientando que esta ferramenta, assim como o *CallerIp* que pertence a mesma fabricante, também não possui o uso gratuito e código-fonte aberto.

4.3 XPLICO

Xplico é uma Ferramenta de Análise Forense de Rede (NFAT - *Network Forensic Analysis Tool*) cujo objetivo é extrair de um tráfego de *internet* capturado ou rede local e seus protocolos como: HTTP, SIP[13], IMAP[14], POP[15], SMTP, TCP, UDP, IPV4[16], IPV6[17] e outros,

[13] *Session Initiation Protocol.*

[14] *Internet Message Access Protocol*

arquivos pcap (*Packet Capture Data Format*) obtidos por ferramentas de captura de tráfego de dados ou aquisição em tempo real para análise (VIEIRA, 2011). A ferramenta realiza o processamento, extração, classificação e disponibilização de informações de protocolos de arquivos de tráfego de redes, sendo que não possui a função de analisador de protocolos de rede como o *Wireshark*[18]. (GALVÃO, 2011, p. 3).

Tendo como principal característica a capacidade de extração do conteúdo a partir de um arquivo pcap, essa ferramenta pode, por exemplo, extrair todos os *e-mails* transportados pelos protocolos POP, IMAP e SMTP, todo o conteúdo transportado pelo protocolo HTTP, todas ligações de VoIP[19], e ainda o conteúdo dos protocolos FTP, TFTP (*Trivial File Transfer Protocol*), entre outros (LIMA, 2010).

O *Xplico* é uma ferramenta estritamente disponibilizada para a plataforma Linux e é liberada sob a licença GNU - GPL sendo que alguns scripts utilizam a licença *Creative Commons Licence* CCBY-NC-AS 3.0 e possui as seguintes características conforme Xplico (2016a):

- Protocolos suportados: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6, entre outros;
- Porta Independente Protocolo de Identificação (PiPi) para cada protocolo de aplicação;
- *Multithreading*;
- Saída de dados e informações em banco de dados SQLite ou banco de dados MySQL e/ou arquivos;
- TCP ACK (*Acknowledgement*) remontagem com a verificação de qualquer pacote;
- A consulta reversa do DNS dos pacotes DNS contidas nos arquivos de entradas, não do servidor DNS externo;

---

[15] *Post Office Protocol*

[16] *Internet Protocol version 4*

[17] *Internet Protocol version 6*

[18] "*Wireshark* é um analisador de protocolo que permite que você capture e navegue interativamente no tráfego de uma rede de computadores em tempo de execução usando a interface de rede do computador" (BRITO, 2012).

[19] *Voice Over IP*

- Não há limite de tamanho para entrada de dados ou o número de arquivos de entrada (o único limite é o tamanho do HD);
- Suporte a IPv4 e IPv6;
- Modularidade. Cada componente *Xplico* é modular. A interface de entrada, o decodificador do protocolo e a interface de saída (*dispatcher)* são todos módulos;
- Capacidade de organizar os dados extraídos da forma mais adequada para a análise do usuário.

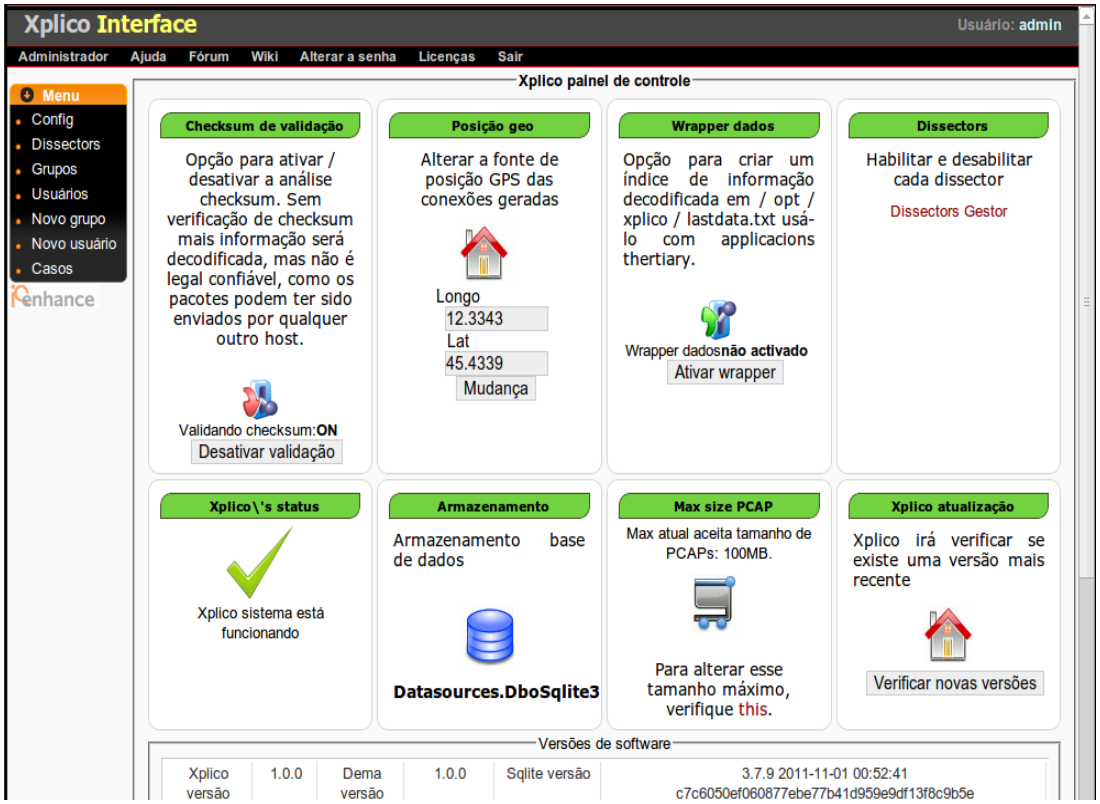
Galvão (2011) comenta que o sistema da ferramenta *Xplico* é composto por quatro macros componentes:

- Gerenciador de decodificadores: *Decode Manager* (DeMa) que organiza a entrada de dados, configura os arquivos de histórico e executa e controla os decodificadores e manipuladores;
- IP *Decoder* Chamado *Xplico* que possui módulos de captura e dissecação dos arquivos pcap;
- Conjunto de Manipuladores de Dados;
- Sistema de Visualização para exibir os dados extraídos.

Para a criação do sistema do *Xplico* foram utilizadas as linguagens de programação C, Python, PHP[20], JavaScript (XPLICO, 2016b). O *software* possui uma interface web criada em linguagem PHP que exibe todo material decodificado pela ferramenta, esta interface pode utilizar um banco de dados SQLite ou MySQL. A Figura 7 evidencia o painel de controle da ferramenta:

[20] *Personal Home Page*

Figura 7: Painel de controle do Xplico



Fonte: FONSECA (2012).

Toda a instalação do *Xplico* é realizada por linha de comando, no entanto a ferramenta possui também uma versão *VirtualBox Image* que contém uma máquina virtual instalada com o *software* instalado e configurado (XPLICO, 2016c).

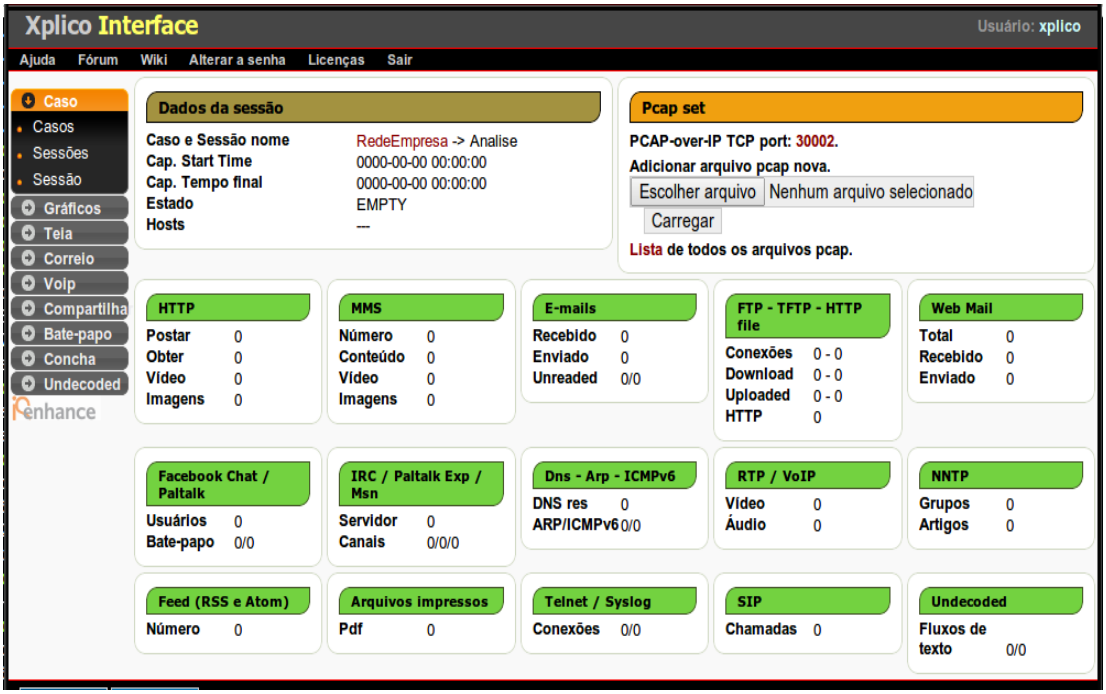
O *Xplico* ainda possui alguns recursos adicionais opcionais, tais como:

- GeoIP C API / GeoLite City database: Visualização Geográfica e temporal de tráfego;
- GhostPCL: reconstrução de documentos enviados para impressão em rede;
- Videosnarf: decodificação de tráfego VoIP baseado no protocolo RTP[21] (GALVÃO, 2011, p. 11).

A Figura 8 mostra a tela de início de uma sessão da ferramenta *Xplico:*

[21] *Real-time Transport Protocol*

Figura 8: Início de sessão de Xplico



Fonte: FONSECA (2012).

4.4 ENCASE FORENSIC

A ferramenta estudada nesse item não é específica para análise de redes, realizando também outros papeis importantes dentro da forense computacional. A seguir serão evidenciados esses atributos que tornam essa ferramenta muito eficaz quando se trata de busca por evidências digitais e criação de laudos íntegros.

Devido a sua característica não tão invasiva o *EnCase Forensic* é uma das ferramentas mais utilizadas pelos peritos forenses na busca por evidências em um ato criminoso. Comumente adotada pelas instituições governamentais e aplicada também em investigações militares, a ferramenta mostra-se vantajosa quando o assunto trata-se de segurança e integridade das evidências. A ferramenta tem a capacidade de realizar análise simultânea de múltiplas máquinas em uma rede LAN/WAN em nível de disco e memória, analisar múltiplas plataformas, identificar dlls (*Dynamic-Link Library*) injetadas no sistema, identificar processos ocultos entre outros. Outra vantagem notória desta ferramenta é a de

proporcionar ao usuário relatórios minuciosos do conteúdo abordado em um nível de aceitação legal para serem utilizados em processos judiciais (GOLDMAN, [S.d.], p. 16).

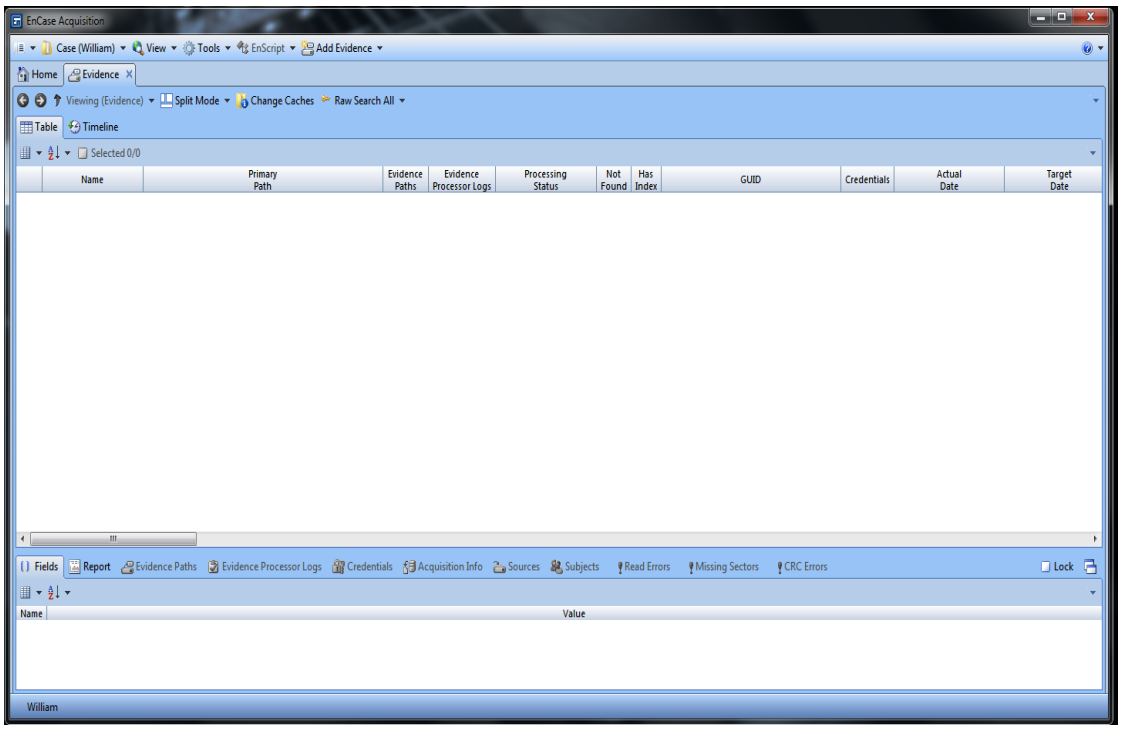
Vargas (2007) salienta que a ferramenta *EnCase* é uma das mais completas quando o assunto trata-se de perícia forense computacional, o autor justifica sua afirmativa baseado nos seguintes pontos:

- Padronização de laudos periciais;
- Organização do banco de dados ligado às evidências;
- Fornece senhas ou as quebra;
- Recuperação de arquivos excluídos.

A ferramenta possui características que deixam sua interface com um grau de dificuldade baixo, facilitando a navegação em seu conteúdo (VARGAS, 2011b).

A seguir a Figura 9 evidencia a tela inicial do *EnCase Forensic*:

Figura 9: Tela inicial do Encase Forensic



Fonte: GUIDANCE SOFTWARE ([199-]e).

Segundo a fabricante Guidance Software ([199-]a) a ferramenta traz consigo um processador de evidências que permite, basicamente, realizar consultas com mais agilidade, automatizar tarefas, criar vários perfis para cada caso e processar arquivos com mais velocidade. Vargas (2011b) menciona que esse processador tem a capacidade de preparar um caso por meio "[...] da realização de tarefas de processamento de chave, tais como a criação de um índice, a análise de *hash*, a análise de assinaturas, a análise de arquivo protegido, internet e processamento de e-mail, e pesquisando palavras-chave". O mesmo autor denota mais alguns recursos do processador de evidências do *Encase Forensic*:

- Realiza análise de arquivos protegidos utilizando-se de um módulo analisador de criptografia;
- Detecta automaticamente informações do sistema operacional;
- Possui um módulo que analisa os arquivos da lixeira, arquivos de *log* e transações MFT (*Master File Table*);
- Possui um localizador e analisador de conversas de bate-papo na internet registradas no sistema;
- Possui um analisador de *logs de* eventos e informações de *login.*

O *EnCase Forensic* possibilita também, através de utilitários internos, identificar arquivos criptografados e protegidos com senha, localizar conversas em mecanismos de bate-papo, localizar *logs* e proporcionar ao usuário a análise de forma abrangente dos arquivos contidos na lixeira e arquivos de *link* (VARGAS, 2011b).

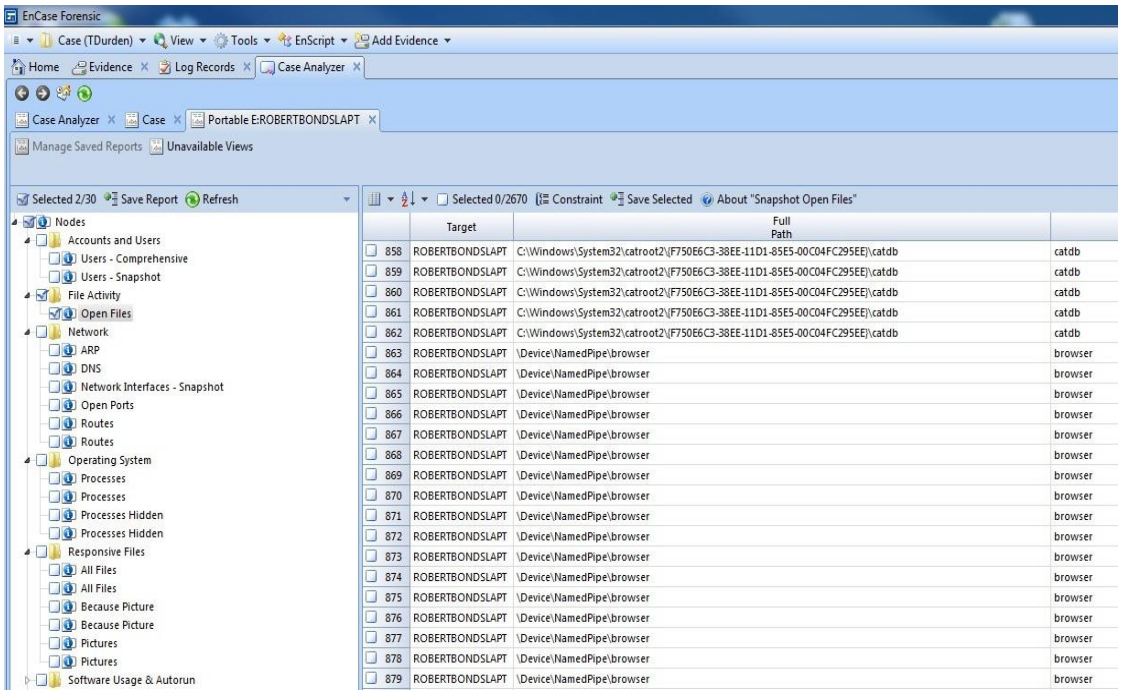
Esta ferramenta capacita o usuário a encontrar milhares de arquivos através de buscas integradas de forma a encontrar uma potencial evidência para a futura análise (GUIDANCE SOFTWARE [199-]b).

Sendo possível a realização de análise de evidências através do *Encase Forensic*, pode-se determinar se um crime pode ou não ter sido cometido. A análise das evidências proporcionada por esta ferramenta visa informar principalmente onde os dados foram criados, por qual motivo aparente o usuário os criou e qual a última data e hora em que os dados foram acessados. A ferramenta oferece ainda ao usuário, principalmente, uma análise avançada dos dados, visualização de fotos e vídeos em diversos formatos, juntada de provas para uma análise mais rápida e permite que o usuário tenha acesso ao que realmente aconteceu no

sistema operacional do computador, podendo assim, fornecer relatórios consistentes. (GUIDANCE SOFTWARE [199-]c).

A Figura 10 mostra a tela de análise do *Encase Forensic*:

Figura 10: Tela de análise do Encase Forensic



Fonte: GUIDANCE SOFTWARE ([199-]e).

Os relatórios disponibilizados por essa ferramenta buscam oferecer ao usuário, principalmente detalhes da informação a ser apresentada, disponibilidade de exportação da informação em arquivos com formatos diferenciados, inclusão de comentários ou opiniões pertinentes do perito e personalização dos relatórios de acordo com o público abordado (GUIDANCE SOFTWARE [199-]d). Esta ferramenta não possui licença gratuita para a sua utilização tampouco o código-fonte aberto.

5. CONSIDERAÇÕES FINAIS

Neste capítulo são apresentadas as considerações finais e recomendações para trabalhos futuros.

5.1 CONSIDERAÇÕES FINAIS

Entre os muitos reflexos da globalização no mundo que aproxima, positiva ou negativamente, as pessoas e instituições pôde-se perceber o surgimento e, posteriormente, o crescimento exponencial de crimes ligados ao mundo digital. Em especial a *internet*, que faz esse papel de aproximação, tornou-se o principal campo de atuação de comunicação entre todo o mundo, fazendo com que pessoas más intencionadas, usando da sensação de anonimato e baixa exposição na rede, desenvolvessem técnicas para a prática de crimes nesse meio. É importante ressaltar que o campo virtual pode ser meio e/ou fim para a prática de crimes.

Diante da problemática explanada, o presente estudo teve como objetivos enveredar-se por campos relacionados ao acometimento do crime virtual dentro da rede de computadores. Para este fim, tornou-se imprescindível que para o alcance dos objetivos fossem necessários conhecer, em princípio, o modo como acontece a comunicação na rede de computadores. Para isso, foram necessárias a conceituação da rede de computadores e a explanação do surgimento da internet e do conjunto de protocolos TCP/IP que possibilitou essa compatibilidade e unificação das redes para a integração de uma grande malha que conecta o mundo.

Em seguida, como modo de agregar à rede de computadores formas de segurança e evidenciar modelos de ataques ao usuário ou à informação, foi tratado do tema Segurança da Informação que destacou métodos fundamentais à garantia dos três principais elementos do

tema compreendido: integridade, confidencialidade e disponibilidade. À vista disso, mediante a quebra desses elementos por causas humanas propositais com a finalidade de prejudicar algo ou alguém, entrou em cena a figura do crime virtual. E diante desse cenário foi substancial que se conceituasse distinguindo as formas em que ocorrem o crime virtual: própria e imprópria. Foi também necessária a exposição da legislação específica atual e a deficiência do poder legislativo em acompanhar a evolução do crime virtual.

Por fim, objetivando a conclusão do escopo desse trabalho, perpassou-se pela forense computacional, onde foi demonstrado as fases dessa ciência forense particular à análise, identificação de indícios e constituição de laudos comprovativos nos casos de ocorrência do ilícito virtual. Ademais, foram demonstradas algumas ferramentas utilizadas na perícia forense computacional capazes de buscar indícios e informações direcionadoras para a investigação dos crimes ocorridos dentro da rede de computadores.

Diante dos fatos apresentados nesse estudo, percebeu-se a relevância na construção e consolidação de conhecimentos específicos sobre determinadas áreas pouco difundidas na sociedade. A dimensão do que envolve o crime virtual e as formas de investigação da polícia, bem como a perícia forense computacional, certamente estão em um grau de complexidade muito além do que esse estudo expôs, contudo, sem dúvidas o conhecimento aqui difundido foi de grande valia para a percepção do que está acontecendo no que se refere aos desdobramentos das ciências diretas e transversais ao estudo do crime virtual na rede de computador.

Este estudo destacou o mérito da forense computacional como modelo de direcionamento de decisões judiciais através da formulação de laudos probatórios. Muito embora, tenha-se evidenciado ferramentas (*softwares*) no mínimo capazes de dar apontamentos direcionadores para a investigação forense, não se imagina a forense computacional como uma ciência exata pautada em métodos formais de investigação, pelo contrário, muitas vezes tem que se recorrer a procedimentos empíricos e de certa forma pontuais e peculiares ao investigador, observando a relevância de sempre preservar a prova. No entanto, isso não necessariamente é uma deficiência, mas sim uma característica a ser absorvida.

Dado o exposto, também é importante que a legislação sempre esteja a se adequar empreendendo esforços na criação de leis locais, nacionais e internacionais e criando métodos

e procedimentos padrão na área da ciência forense computacional aceitos internacionalmente, pois como se sabe o mundo virtual não possui fronteiras.

5.2 RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Com base no estudo apresentado, recomenda-se para trabalhos futuros:

- Aprofundamento sobre o tema crime virtual evidenciando a Legislação e acordos internacionais em que o Brasil está inserido e formas de obter informações junto aos servidores internacionais;
- Demonstração de ferramentas forenses para a obtenção de dados em unidades de armazenamento e criação de código *hash*.

6. REFERÊNCIAS

ALECRIM, Emerson. **Vírus de computador e outros malwares:** o que são e como agem. Infowester. 2011. Disponível em: <http://www.infowester.com/malwares.php>. Acesso em: 20 nov. 2016.

APARÍCIO, Nuno. **Redes de comunicação**. 2012. Disponível em: <http://redesecomunicacaonuno11i.blogspot.com.br/2012/12/modelo-tcpip.html>. Acesso em: 10 ago. 2016.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BRASIL. **Curso Crimes Cibernéticos:** procedimentos básicos. SENASP/MJ, 2016.

_____. **LEI Nº 9.609, de 19 de fevereiro de 1998.** Brasília: Diário Oficial da União, 1998. Disponível em: <http://www.amperj.org.br/store/legislacao/leis/L9609_leisoftware.pdf>. Acesso em: 06 jan. 2017.

_____. **LEI Nº 11.829, de 25 de novembro de 2008.** Brasília: Diário Oficial da União, 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em 06 jan. 2017.

_____. **LEI N°12.735, de 30 de novembro de 2012**. Brasília: Diário Oficial da União, 2012. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 05 jan. 2017.

_____. **LEI N°12.737, de 30 de novembro de 2012**. Brasília: Diário Oficial da União, 2012a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 05 jan. 2017.

_____.**LEI Nº12.965, de 23 de abril de 2014**. Brasília: Diário Oficial da União, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 jan. 2017.

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança:** o guia oficial RSA. Rio de Janeiro: Elsevier, 2002.

BRITO, Edivaldo. **Como usar o wireshark.** 2012. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2012/09/como-usar-o-wireshark.html>. Acesso em: 15 mar. 2017.

CAGNANI, Caio; SANTOS, Valdecir de Deus dos. **Computação forense:** fundamentos. [2007?]. Disponível em: <http://pt.scribd.com/doc/47774532/computacao-forense-fundamentos>. Acesso em: 09 fev. 2017.

CANDIDO JUNIOR, Arnaldo; SAÚDE, Almir Moreira. **Técnicas e ferramentas utilizadas em análise forense**. 2005. Disponível em: <ftp://ftp.registro.br/pub/gts/gts0205/05-tech-tools-forensics.pdf>. Acesso em: 08 de fev. 2017.

CARVALHO, Hugo Eiji Tibana. **PKI – infra-estrutura de chaves públicas.** 2008. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/Anos-anteriores/2008-2/trabalhos_vf/hugo/index.html>. Acesso em: 20 nov. 2016.

CIPOLI, Pedro. **O que é engenharia social.** Canaltech. 2012. Disponível em: <http://corporate.canaltech.com.br/o-que-e/seguranca/O-que-e-Engenharia-Social/>. Acesso em: 20 nov. 2016.

COSTA, Marco Aurélio Rodrigues da. **Crimes de informática.** Jus Navigandi**.** 1995. Disponível em: <http://jus.com.br/artigos/1826/crimes-de-informatica/2>. Acesso em: 6 maio 2016.

DUMAS, Véronique. A origem da internet. **História viva**. Reportagem. 2013. Disponível em: <http://www2.uol.com.br/historiaviva/reportagens/o_nascimento_da_internet.html>. Acesso em: 24 abr. 2016.

FERREIRA, Gecivaldo Vasconcelos. **Teoria do crime em síntese**. Jus Navigandi. 2008. Disponível em: <http://jus.com.br/artigos/10913/teoria-do-crime-em-sintese>. Acesso em: 01 maio 2016.

FERREIRA, Lóren Pinto. **Os "crimes de informática" no direito penal brasileiro**. [2009]. Disponível em: <http://www.oab.org.br/editora/revista/revista_08/anexos/crimes_de_informatica.pdf>. Acesso em: 20 mar. 2016.

FONSECA, Vagner. **Análise de tráfego de rede**. 2012. Disponível em: <http://www.cooperati.com.br/2012/10/18/analise-de-trafego-de-rede/>. Acesso em: 15 mar. 2017.

FONTES, Edson. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

FORTES, Carlos José e Silva. **Lei 11.829/2008 – Combate à pornografia infantil e pedofilia criminosa**. [2008]. Disponível em: <http://www.devoltapracasa.org.br/index.asp?c=paginas&modulo=informativo_exibe&url=166>. Acesso em: 04 jan. 2017.

FREITAS, Andrey Rodrigues. **Perícia forense aplicada à informática**. 2003. Disponível em: <http://www.linuxsecurity.com.br/info/general/andrey-freitas.pdf>. Acesso em: 07 fev. 2017.

_____. **Perícia forense aplicada à informática:** ambiente Microsoft. Rio de Janeiro: Brasport, 2006.

GALO, Carlos Henrique. **Lei nº 12.695/11:** o marco civil da internet – análise crítica. [2014]. Disponível em: < https://henriquegalo.jusbrasil.com.br/artigos/118296790/lei-n-12965-11-o-marco-civil-da-internet-analise-critica>. Acesso em: 25 jan. 2017.

GALVÃO, Ricardo Kléber Martins. **Análise de tráfego de redes com Xplico.** 2011. Disponível em: <http://www.ricardokleber.com/palestras/2011_12_02_-_HacknRio2011_-_Analise_De_Trafego_de_Redes_com_Xplico.pdf>. Acesso em: 15 mar. 2017.

GOLDMAN, Alfredo. **Artigo sobre computação forense**. [S.d.]. Disponível em: <http://grenoble.ime.usp.br/~gold/cursos/2008/movel/gradSemCorrecao/FelipeBulleC.pdf>. Acesso em: 18 mar. 2017.

GOMES, Olavo José Anchieschi. **Segurança total**. São Paulo: Makron Books, 2000.

GONÇALVES, Márcio. et al. Perícia forense computacional: metodologias, técnicas e ferramentas. **Revista Científica Eletrônica de Ciências Sociais Aplicadas da Eduvale**. Jaciara, MT. a. V, n. 07, nov./2012, p. 1-17. Disponível em: < http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf >. Acesso em 21 mar. 2016.

GUERRA, Ráisa. **O que é spam**.Tecmundo. 2012. Disponível em: <http://www.tecmundo.com.br/spam/223-o-que-e-spam-.htm>. Acesso em: 220 nov. 2016.

GUIDANCE SOFTWARE. **EnCase Forensic:** Process. [199-]a. Disponível em: <https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Process.aspx>. Acesso em: 18 mar. 2017.

_____. **EnCase Forensic:** Search. [199-]b. Disponível em: <https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx>. Acesso em: 18 mar. 2017.

_____. **EnCase Forensic:** Analyze. [199-]c. Disponível em: <https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Search.aspx>. Acesso em: 18 mar. 2017.

_____. **EnCase Forensic:** Report. [199-]d. Disponível em: <https://www.guidancesoftware.com/products/Pages/EnCase-Forensic/Report.aspx>. Acesso em: 18 mar. 2017.

_____. **EnCase Forensic.** V7.[199-]e. Disponível em: <http://www.4shared.com/file/SvG0066A/encaseforensic-v702-en.html>. Acesso em: 18 mar. 2017.

HAMANN, Renan. **O que um antivírus precisa ter para ser eficiente?** Tecmundo. 2010. Disponível em: <http://www.tecmundo.com.br/seguranca/3663-o-que-um-antivirus-precisa-ter-para-ser-eficiente-.htm>. Acesso em: 20 nov. 2016.

HAYDEN, Matt. **Aprenda em 24 horas redes**. Rio de Janeiro: Campus, 1999.

INFORMAL, Dicionário. **Modus operandi.** Dicionário Informal. 2010. Disponível em: <http://www.dicionarioinformal.com.br/significado/modus%20operandi/7370/>. Acesso em: 5 dez. 2016.

ITI. **O que é certificado digital.** [S.d.]. Disponível em: < http://www.iti.gov.br/certificacao-digital/o-que-e>. Acesso em: 20 nov. 2016.

HAYDEN, Matt**. Aprenda em 24 horas redes**. Rio de Janeiro: Campus, 1999.

KARASINSKI, Eduardo. **Segurança:** como confiar nos certificados digitais?. Tecmundo. 2009. Disponível em: <http://www.tecmundo.com.br/web/2677-seguranca-como-confiar-nos-certificados-digitais-.htm>. Acesso em: 20 nov. 2016.

KLEINA, Nilton. **Agora é oficial:** lei Carolina Dieckmann é aprovada por Dilma Rousseff. Tecmundo. 2012. Disponível em: <http://www.tecmundo.com.br/projeto-de-lei/33567-agora-e-oficial-lei-carolina-dieckmann-e-aprovada-por-dilma-rousseff.htm>. Acesso em 04 jan. 2017.

KOLLING, Gabriella S. **Segurança da informação.** [2010]a. Disponível em: <http://seguranca-da-informacao.info/>. Acesso em: 20 nov. 2016.

_____. **Ameaças à segurança do computador.** [2010]b. Disponível em: <http://seguranca-da-informacao.info/mos/view/Amea%c3%a7as_%c3%a0_Seguran%c3%a7a_do_Computador/>. Acesso em: 20 nov 2016.

_____. **Soluções.** [2010]c. Disponível em: <http://seguranca-da-informacao.info/mos/view/Solu%C3%A7%C3%B5es/>. Acesso em: 20 nov 2016.

_____. **Criptografia.** [2010]d. Disponível em: <http://seguranca-da-informacao.info/mos/view/Criptografia/>. Acesso em: 20 nov. 2016.

LIMA, Gustavo. **Xplico 0.6.0:** Uma ferramenta que dá um plus ao que foi capturado pelo Wireshark. 2010. Disponível em: <http://blog.corujadeti.com.br/xplico-0-6-0-uma-ferramenta-que-da-um-plus-ao-que-foi-capturado-pelo-wireshark/>. Acesso em: 15 mar. 2017.

MARCELO, Antonio; PITANGA, Marcos. **Honeypots:** a arte de iludir hackers. Rio de Janeiro: Brasport, 2003.

MARTINS, Elaine. **O que é esteganografia?** Tecmundo. 2010. Disponível em: <http://www.tecmundo.com.br/video/3763-o-que-e-esteganografia-.htm>. Acesso em: 20 nov. 2016.

_____. **O que é um Worm.** Tecmundo. 2008. Disponível em: <http://www.tecmundo.com.br/antivirus/206-o-que-e-um-worm-.htm>. Acesso em: 09 nov. 2016.

_____. **O que é VPN?** Tecmundo. 2009. Disponível em: <http://www.tecmundo.com.br/1427-o-que-e-vpn-.htm>. Acesso em: 21 nov. 2016.

NASCIMENTO, Nelson José do. **Ameaças e vulnerabilidades da informação**: como precaver. Portal Educação. 2013. Disponível em: <http://www.portaleducacao.com.br/educacao/artigos/48819/ameacas-e-vulnerabilidades-da-informacao-como-precaver>. Acesso em: 09 nov. 2016.

OLIVEIRA, Luiz Gustavo Caratti; DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real**. Âmbito jurídico. 2011. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963>. Acesso em: 04 jan. 2017.

OLIVEIRA, Sabrina Vitório. **Pericia forense em sistemas GNU/LINUX**. 2007.79 f. (Monografia) Faculdade Salesiana de Vitória, Vitória: 2007. Disponível em: <http://www.multicast.com.br/sergio/arquivos/monografia-pos-seguranca-pericia-forense.pdf>. Acesso em: 08 fev. 2017.

PINHEIRO, Emeline Piva**. Crimes virtuais**: uma análise da criminalidade informática e da resposta estatal. [2006?]. Disponível em: <http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2006_1/emeline.pdf>. Acesso em: 20 abr. 2016.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. **O problema na tipificação penal dos crimes virtuais**. Jus navigandi. 2002. Disponível em: <http://jus.com.br/artigos/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais/1>. Acesso em: 22 abr. 2016.

REIS, Marcelo Abdalla dos; GEUS, Paulo Lício de. **Análise forense de intrusões em sistemas computacionais:** técnicas, procedimentos e ferramentas. [2002?]. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2002-Pericia-marcelo.reis-forense.tecnicas.procedimentos.pdf>. Acesso em: 07 fev. 2016.

ROCHA, Luiz Carlos. **Investigação policial:** teoria e prática. 2. ed. São Paulo: Edipro, 2003.

ROSA, Ana Paula Teixeira. Forense de memória: extração e análise de dados armazenados em memória volátil. 2011. Disponível em: <http://www.peotta.com/arquivos/forense/Monografia_AnaPaula_UnB_vFinal.pdf>. Acesso em: 09 fev. 2017.

SANTOS, Altamiro J. dos**. Direito de segurança pública e legítima defesa social**. São Paulo: LTr, 2006.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação aplicada ao Security Officer. Rio de Janeiro: Elsevier, 2003.

SERAFIM, Higor Mancilha Vantuil; LISBOA, Miriam Senise. **Princípio da segurança cibernética**. Jus Navigandi. 2014. Disponível em: <http://jus.com.br/artigos/27977/principio-da-seguranca-cibernetica>. Acesso em: 04 jan. 2017.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos tribunais, 2003.

SHIPLEY, Todd; BOWKER, Art. **Investigating internet crimes**: an introduction to solving crimes in cyberspace. 1 ed. Waltham: Elsevier, 2014.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio**. Redes de computadores**: das LANs, MANs e WANs às redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

SÔNEGO, Arildo. **Auditoria e segurança de sistemas**. Faculdades ESUCRI. Material de aula. 2012.

STAIR, Ralph; REYNOLDS, George W. **Princípios de sistemas de informação**: uma abordagem gerencial. São Paulo: Pioneira Thomson Learning, 2006.

STALLINGS, William. **Criptografia e segurança de redes**.4. ed. São Paulo: Pearson Prentice Hall, 2008.

TANENBAUM, Andrew S. **Redes de computadores**. Rio de Janeiro: Campus, 1997.

_____. **Redes de computadores**. Rio de Janeiro: Elsevier, 2003.

THOMAS, Tom. **Segurança de redes:** primeiros passos. Rio de Janeiro: Ciência Moderna, 2007.

VARGAS, Raffael. **Perícia forense computacional:** ferramentas periciais. Gerência de TI. 2007. Disponível em: <http://imasters.com.br/artigo/6485/gerencia-de-ti/pericia-forense-computacional-ferramentas-periciais/>. Acesso em: 14 mar. 2017.

_____. Perícia Forense Computacional Metodologias e Ferramentas Periciais. **Evidência Digital Magazine.** 2011a. Disponível em: <http://www.guiatecnico.com.br/evidenciadigital/Downloads/Evidencia_Digital_05.zip>. Acesso em 14 mar. 2017.

_____. **Conhecendo o EnCase Forensic V7**. Imasters. 2011b. Disponível em: <http http://imasters.com.br/artigo/21358/gerencia-de-ti/conhecendo-o-encase-forensic-v7/>. Acesso em: 18 mar. 2017.

VIEIRA, Vinícius. **Xplico**: uma ferramenta de análise forense de redes. 2011. Disponível em: <http://sejalivre.org/xplico-uma-ferramenta-de-analise-forense-de-redes/>. Acesso em: 15 mar. 2017.

VISUALWARE. **CallerIP IP and port monitoring.** 2014a. Disponível em: <http://www.callerippro.com/detail.html>. Acesso em: 11 mar. 2017.

_____. **CallerIP user interface.** 2014b. Disponível em: <http://www.callerippro.com/support/v4/gui.html>. Acesso em: 11 mar. 2017.

_____. **CallerIP IP plots the IP origin on a world map.** 2014c. Disponível em: <http://www.callerippro.com/iporigin.html>. Acesso em: 12 mar. 2017.

_____. **CallerIP IP relatórios Whois.** 2014d. Disponível em: <http://www.callerippro.com/whois.html>. Acesso em: 12 mar. 2017.

_____. **CallerIP Connection History.** 2014e. Disponível em: <http://www.callerippro.com/support/v4/conhist.html>. Acesso em: 12 mar. 2017.

_____. **CallerIP History Log Search.** 2014f. Disponível em: <http://www.callerippro.com/support/v4/history.html>. Acesso em: 13 mar. 2017.

_____. **Menus CallerIP.** 214g. Disponível em: <http://www.callerippro.com/support/v4/menus.html>. Acesso em: 13 mar. 2017.

_____. **CallerIP**, 4.1b (Build 3275). 2014h. Disponível em: <http://www.baixaki.com.br/site/dwnld17653.htm>. Acesso em: 13 mar. 2017.

_____. **Emailtrackerpro.** 2014i. Disponível em: <http://www.emailtrackerpro.com/index.html>. Acesso em: 14 mar. 2017.

_____. **Emailtrackerpro:** trace the header or the email address. 2014j. Disponível em: <http://www.emailtrackerpro.com/support/v10/headeroraddress.html>. Acesso em: 14 mar. 2017.

_____. **Emailtrackerpro:** performing a trace**.** 2014k. Disponível em: <http://www.emailtrackerpro.com/support/v10/traceemail.html>. Acesso em: 14 mar. 2017.

_____.**Emailtrackerpro**, 10.0a (Build 4058). 2014l. Disponível em: <http://www.baixaki.com.br/download/emailtrackerpro.htm>. Acesso em: 14 mar. 2017.

XPLICO. **About.** 2016a. Disponível em: <http://www.xplico.org/about>. Acesso em: 15 mar. 2017.

_____. **Docs.** 2016b. Disponível em: <http://www.xplico.org/docs>. Acesso em: 15 mar. 2017.

_____. **Xplico version.** 2016c. Disponível em: <http://www.xplico.org/download>. Acesso em: 15 mar. 2017.